An integrative model of information security and trust in socio-technical environments

Greaves, Duncan

Award date:
2020

An integrative model of information security and trust in socio-technical environments.

By

Duncan J. Greaves

PhD

July 2019

Acknowledgements

It has been an unconventional route towards the completion of this PhD thesis, a long, winding and colourful road that has tested the resolve of many of the contributors. I thank you all for your input, insight and support throughout.

Firstly, I would like to thank the Centre for Business in Society at Coventry University for the opportunity that they have given me. I am grateful to the academic, operations and administrative staff who regularly go above and beyond to enable myself and others to succeed. Coventry University has a vibrant research community, and my fellow postgraduate researchers have made my PhD study an absolute pleasure.

I owe a massive debt of gratitude to both of my supervisors whom I consider to be firm friends and colleagues.

I would especially like to thank my Director of Studies, Dr Harjit Sekhon who has pushed and guided me towards my goals throughout. I would like to thank him for sharing the wisdom of his experience, including classic non-attributable quotes like *"the difference between trust and blind faith is like the difference between Liverpool FC and Leeds United"*.

I would also like to thank my supervisor Dr Alexeis Garcia-Perez for sharing his mastery of the technical and knowledge management side of things, and for always stepping in at the right time with the correct guidance.

I would like to thank many of my past employers for allowing me to mess up their computer systems in the name of scientific research. These include Ann Whaley at Yorkshire Water, Haydn Smith at Vaultex UK, Marc Kirk at Seven Seas, and Barbara Richardson at Pearson Edexcel. Although none of us realised it at the time it set in motion a research odyssey that has culminated in this work.

Many thanks to Dr Seth Giddings and Rob Farley who wrote glowing references to start the whole thing off, as well as my old school classmates, colleagues and housemates who have shown support, mainly by buying me drinks.

I would also like to thank my brothers, Dr Alan Greaves and Prof David Greaves for acting as informal supervisors, their partners Ganesh and Stephanie and my daughters Daisy and Holly for their support throughout, especially through the medium of good food.

Last but not least, to my mum, for all of the unconditional love, companionship and support that she has given to me in my studies. It is fair to say I could not have done this without you. I would also like to think that my dad, Jack Greaves, who is sadly no longer with us, would also be proud, and probably amused, at this unorthodox route to finishing my homework.

Abstract

The need for cybersecurity measures is evidenced by the myriad information security and digital trust breaches in modern socio-technical systems. The need to understand and counteract the uncertainty and risk associated with trust in digital environments triggered this research. The enquiry explored the role of information security in the formation of trust relationships and the extent to which it influences the production of trust.

A mixed methods design incorporated the development of a 45-item scaled survey instrument. Data were collected from 405 members of the UK general public using an online questionnaire and were analysed using exploratory factor analysis (EFA), confirmatory factor analysis (CFA) and structural equation modelling (SEM) to validate the research model and to test the research hypotheses.

The findings revealed that information security has a strong relationship with reputation, a key mediating factor in both task delegation and trust formation. Trust is also shown to have a strong relationship with communication quality and influences behavioural outcomes. The findings are stable across the three research contexts of Retail, Banking and Healthcare that were investigated.

This research extends the Theory of Planned Behaviour to include information security as a component of perceived behavioural control, and extends the Social Exchange Theory to include an appreciation of security values as motivation for reciprocated trust relationships.

The management implications of this work include insights into the role of information security in organisational reputation building and outlines several possible avenues for further academic research.

Publications Associated with this Thesis

Duncan Greaves (2019) Making Sense of Big Data Using Cluster Analysis, Impact, 2019:1, 25-29, May 2019.

Data, Organisations & Society Conference, Coventry University "Tensions between Structure and Agency: The organisational challenges of cybersecurity", Nov 2018.

25th Computer Security Symposium and SABSA World Congress (COSAC), Ireland. "The Architecture of Trust and its' Security Implications", Oct 2018.

Behavioural and Social Sciences in Security, Lancaster University, #BASS18. "Information flow and trust formation in socio-technical systems", July 2018.

2018 AMS World Marketing Congress, Lusãada University of Porto, Portugal, "Trust and Cyber Security in Big Data Systems", June 2018. (Paper accepted, but unable to attend and present due to illness.)

Table of Contents

List of Tables

List of Figures

List of Abbreviations

CFA	Confirmatory Factor Analysis
EFA	Exploratory Factor Analysis
SEM	Structural Equation Modelling
CB-SEM	Covariance Based Structural Equation Modelling
MLE	Maximum Likelihood Estimation Method
RTR	Risk Taking Relationship
ANOVA	Analysis of Variance
GDPR	General Data Protection Legislation (ICO [1], 2018).
TPB	Theory of Planned Behaviour
MAS	Multi-Agent Systems
PII	Personally Identifiable Information
ML	Machine Learning
AI	Artificial Intelligence
BI	Business Intelligence

An integrative model of information security and trust in socio-technical environments.

By

Duncan J. Greaves

July 2019

A thesis submitted in partial fulfilment of the University's requirements for the Degree of Doctor of Philosophy

1. Introduction

Trust plays a stabilising role in circumstances of uncertainty and risk, situations that neatly characterise the dynamic nature of modern digital commerce and interaction. The confidence of trust inspires the new ways of thinking, co-operation and innovation with which to face and resolve difficult situations. However, trust also demands an environment where the need to monitor or control others is lessened. This becomes a problem in cognitively powered environments where advantage can be gained at the expense of trusting parties.

Consider entering any other situation of risk without controls or protection, such as entering a burning building without breathing apparatus, or driving at speed without a seatbelt on. Applying protective controls gives a feeling of assurance that harm prevention measures are in place, and that the threat will be contained. For example, if you find yourself entering hazardous territory without the power to control risk, then who is doing the protection on your behalf? In situations like wearing

breathing apparatus or a seatbelt the individual is empowered to protect themselves from harm, and legal compulsion and social norms play a large part in guiding individual choice where there are no options that do not require trust. Trust in others to do the right thing lessens the need to monitor compliance, but we should not be naïve about the necessity for protection.

This thesis argues that the responsibility for the well-being and freedom from threat of the participants in the digital environment is that of the trustee organisations and institutions. By acting as the guarantors of trust by implementing environmental controls to protect parties, trustees retain the expectant confidence of users whilst earning a reputation premium for demonstrating this duty of care.

1.1 Background to the Research

This thesis on the social and technical elements of cybersecurity management has relevance and immediacy as evidenced by the myriad information security and digital trust breaches in modern socio-technical systems. This analysis is precipitated by the need to gain an understanding of how the elements that exercise control in socio-technical systems contribute to, or detract from, trusting behaviours and relationships.

Although trust is not necessary for conducting business, the costs of not securing trust information includes loss of customers; failing to attract potential future customers; negative reputation effects; loss of business partners and potential legal

liabilities (Ko and Durantes, 2006). Doing business without trust leads to increased processing and monitoring costs, less speedy decision making, and decreased market capitalisation (Shapiro et al., 1992). Whether with it or without it, trust has a financial impact on the health of organisations. Carried forward to the digital realm, exchanges between parties rely on both trust in the technology and trust in the merchant (Gefen, 2008). Therefore, this enquiry into the nature of the relationship between technology and humans is necessary to inform the both emerging field of cybersecurity and the established field of management.

1.1.1 Research Problem and Rationale

There are several identified gaps in the literature on trust and decision making that are filled by this research enquiry. There is a large body of academic work on the nature of trust and trustworthiness in the field of social sciences that guides the interpretation of trusting behaviour. There is also considerable literature in the fields of computer security and information systems that deal with the vulnerabilities and manifestations of the breaches of security in the digital realm. However, the confluence of these two fields is an area that remains largely unexplored due to the interdisciplinary nature of the interaction between computers and relationship formation.

The key works in trust formation referenced within this thesis are those of Mayer et al. (1995) and McKnight and Chervaney (2002). These works, in turn, draw

on the Theory of Planned Behaviour (TPB), (Ajzen, 1985), in their consideration of psychological states in the trust formation process. Psychological states play a role in the consideration of antecedent belief factors through to a commitment to behaviour. These behaviours are modified into outcomes through the mechanisms proposed in Social Exchange Theory (Blau, 1964) that reinforce the value of trust. The contribution of these scholars to the fields of trust and psychological decision making is central to this enquiry, yet it was not thought necessary in any of these frameworks to mention security. This reveals an oversight from the classical literature that did not exist prior to the widespread introduction of open networks of computer systems. The security between exchange partners was implicit and was not considered widely outside the field of contract (Williamson, 1993). The disintermediation of personal relationships via electronic communication systems has left gaps in the development of theory in an area of growing concern.

The field of cybersecurity lies in a seemingly different realm to that of trust, with its roots in the field of information systems research. Research on cooperative behaviour in the area of multi-agent systems (MAS) has concentrated on the operationalisation of cognitive trust and security (Jøsang et al., 2007; Marsh, 1994), arguably at the expense of understanding the complex relationship between psychology and computing in social settings (Castelfranchi, 2006). As a result, there is no single clear definition of what cybersecurity is (Futter, 2018) and how the operation of machines has a relationship with trust. This thesis addresses the issue of blending

technology and human behaviour by defining the security of information online as it relates to psychological decision making, and producing a novel classification of information system functions as they relate to the psychological drivers to trust.

In considering and joining the two fields of information security and trust the work provides an explanatory framework within which both the probability based concerns of risk and security and the possibility based concerns of trust are accommodated. In doing so, it will add value to both source disciplines by allowing the operationalisation of security controls in the management of trust based information systems. Conversely, it aids system design as it relates to the formation and maintenance of trusting relationships. The criticality of this investigation into the co-dependence of information security and trust is apparent from the data breaches and cybersecurity concerns that affect governments, organisations and individuals. This research aims to fill the gaps between knowledge of information control and information utilisation in the formation of trust.

The approach taken in this research is to link the control variables of information security and reputation to trust formation psychological states using a decision making framework, the TPB. The use of the TPB in studies of information security compliance and violations is not new. A systematic review (Sommestad and Hallberg, 2013) of the subject found that of the sixteen published studies at the time, there was only a single study that addressed all of the variables covered by the theory, and the authors specific recommendation that *"researchers should consider conducting studies*

focusing explicitly on the TPB to further explore and establish its efficacy for predicting and explaining information security behaviour before mixing multiple theories" was followed in this work. The author of the TPB recommended that the theory was open to additional variables where the proposed addition is behaviour specific; is a possible causal factor of behaviour; conceptually different; generally applicable; or explains sufficient variance (Ajzen, 1991). Therefore, extension of the TPB to include information security and reputation as belief forming variables is pertinent in an area of investigation where behavioural explanation of information security echoes the TPB but rarely names it as a driver.

The use of this theory closes other loopholes identified in the literature. Using the ontological approach of modelling psychological states and mapping the supporting information systems to these roles helps to identify the IT artefacts that have the potential to increase trust in e-commerce (Gefen, 2008:281). This brings the field of cybersecurity management a step closer to developing new models to deal with computational trust in cyberspace (de Olivieira Alberquerque et al., 2016). In particular, this work notes prior work on the observed deterioration of reputation and trust in systems that are subjected to cyberattack (Mármol and Pérez, 2009) and seeks to find an explanation of such attacks from the perspective of how the variables are related as part of the decision making framework of the TPB.

1.1.2 Research Questions

Investigation of the research problem objectives were directed by the research questions that were formulated as follows:

- What is the role of information security in the formation of trust in socio-technical environments?
- How does, and to what extent, if any, does information security influence and inform trust online?
- What is the importance and role of trust in behaviour in digital environments?
- Does context moderate the role and effects of information security on trusting behaviour?

To answer these questions relating to the problem, a series of specific, baselined, measurable objectives were formulated, with which to conduct the research effort. These objectives were used to focus the enquiry, to guide goal setting, and to monitor and evaluate progress.

1.1.3 Research Objectives

To address the need for research in this area, the following objectives were set for the research work to:

- Conduct a comprehensive review of the literature as it relates to trust and information security. The aim of the exercise was to critically analyse the nature and role of trust and trustworthiness and the formation of risk taking relationships. The literature review also examined the supporting role of information systems in trust formation, enacting security controls and the effects of cyberattacks on trust formation and behaviour processes.
- Develop a definition of information security as it relates to trust. The aim being to further the understanding of how information systems influence trust forming variables.
- Develop a conceptual model of information security and trust formation, with the aim of making theoretical contribution by further developing the areas of theory underpinning the research work.
- Produce an integrated logical model of information security and trust that was tested using scaled data collected from the UK general public. The aim of testing was to validate and produce evidential support for the existence of the relationships derived from the model.
- Define contexts of cybersecurity concern with which to statistically test the stability and generalisability of the logical research model.

1.1.4 Research Contexts

The enquiry generalised the research model and findings by analysing context as a moderating variable influencing trust and the delegation of trusting tasks and

behaviour. Within the specific organisational structures that support these contexts, trust is a relationship in which delegation is common. It occurs where specialist tasks are needed, like payment, or to access functionality from the trustee organisation. Delegation is a way of operationalising the execution of tasks, and involves the delegated agents acting on behalf of the customer, with or without explicit consent. To ascertain the influence of context on trusting behaviour, three scenarios of trusting task delegation were chosen to highlight differences in the character of trust between them.

- The first context was online retail, which is the largest online sector with a value of £533bn in 2017 and accounted for almost a third of total consumer spending (Statista.com, 2019). As such, it represents a large and diverse potential cyberattack target.
- The second context was online banking. In 2017, £121 million was lost to online fraud in the UK (statista.com, 2018), and total fraud losses to the UK financial services industry in 2016 amounted to £768.8 million (FFAUK, 2017). However, recent research also suggests that banks have the highest trust ratings for information security, especially personal data (nCipher.com, 2019).
- The third context analysed was Healthcare. This sector in the UK is mostly provided by the NHS, where 91.2% of patients have confidence and trust in the last GP they saw (England.nhs.uk, 2018). An incident in 2017 saw over a third of hospitals affected by the WannaCry encryption virus (NAO, 2019) affecting

appointments and patient records. As such, it represents a high interpersonal trust environment where communication system trust is variable.

1.1.5 Research Approach, Methodology and Design.

The approach taken to the investigation used a critical realist research paradigm to investigate the research problem. This was implemented by utilising a mixed, predominantly quantitative, methodology and research methods to analyse the data collected using descriptive and inferential statistics. The research design utilised a card sort exercise and a 32 participant online pilot study to select question item stems prior to the implementation of a full study of 405 UK based questionnaire respondents.

The questionnaire data was analysed using EFA, CFA and SEM techniques to assess the validity of seven research hypotheses. The findings of the study were further generalised by using data relating to the exemplar contexts, and insight into how and when the relationships were in effect was provided by quantitative path analysis using mediation and moderation techniques.

1.2 Key Findings

This thesis makes contributions to theory development and extends knowledge in the field in the following main areas.

It extends Ajzen's (1985) Theory of Planned Behaviour with an appreciation that information security is a perceived behavioural control variable that acts with

reputation to influence the intention of a market participant to trust. It achieves this by empirically demonstrating a strong positive covariance between information security and reputation, and that information security and the delegation of tasks are fully mediated by reputation. The ontological basis for this reasoning is that cybersecurity is a construct outlining the values of the organisation to be trusted that is communicated via reputation.

This thesis also contributes to the Social Exchange Theory by producing evidence that information security contributes to reciprocated exchange by increasing the communication quality and behavioural outcomes from trusting interactions. By considering outcomes separately from delegated action the influence of trust on reciprocal action is isolated as a component that contributes to the relationship.

1.2.1 Theoretical Findings

The research results produced evidence that there is a strong covariance relationship between the effects of information security and the effects on the reputation of an organisation. The findings were stable and consistent across the three contexts of retail, banking and healthcare that were investigated as part of the research. This finding further develops the theory of trust formation from a TPB perspective and positions information security as a key construct in building organisational reputation, and in turn eliciting the delegation of tasks to the organisation.

An additional finding resulting from the analysis was that trust affected the outcomes of behaviour through the modifying effects of communication quality. A positive covariance relationship between trust and outcomes was found to be mediated by communication quality. This finding echoed the prior literature on trust that found there was a positive relationship between co-operation and communication and trusting outcomes (Jarvenpaa and Leidner, 1999; Putnam, 1995). In the socio-technical settings that this relationship was tested, trusting communication was found to be a higher contributor to outcomes than the outputs of delegated action, suggesting that the presence of trust remains an important factor in online relationships.

The research re-affirmed the close relationship between trust and trustworthiness (as reflected in the variable of reputation) described in the academic literature (Hardin 1996; 2002; Sekhon et al., 2014), and also found the two concepts to be sufficiently differentiated in practice to provide strong constructs of trust and reputation with discriminant reliability.

1.2.2 Managerial Findings

Contextual analysis provided both stability and generalisability of the findings to all contexts explored in this research. The domain specific models gave insight into the management of information security and trust relationships in retail, banking and healthcare settings. The key findings for management in practice were that:

- Information security is a context-less variable, and therefore applicable to management in all of the contextual settings investigated.
- The application of information security values produces a reputation dividend that enhances the willingness of individuals to trust and accept the benefits of socio-digital systems in all of the contexts investigated.
- That organisations who appear to value security and whose information security attitudes are shared with those of customers are likely to gain higher levels of delegated action. The delegated actions can be either trusted or untrusted, with trusted actions increasing the positive outcome effects of delegation.

The research highlights the importance of information security in trust, and the enhancement of reputation that comes with informing potential customers of the values that underpin the security stance of an organisation. This finding implies that capital expenditure on information security controls is an investment in reputational measures. This is in opposition to the prevailing business view that information security controls represent a financial loss to the organisation.

1.3 Thesis Structure

This thesis is aligned to a standard format for investigative work of this type, and consists of the chapters shown in Figure 1-1. The sections and coverage of each chapter are detailed in the thesis structure shown in Table 1.1.

Figure 1-1 Thesis Map

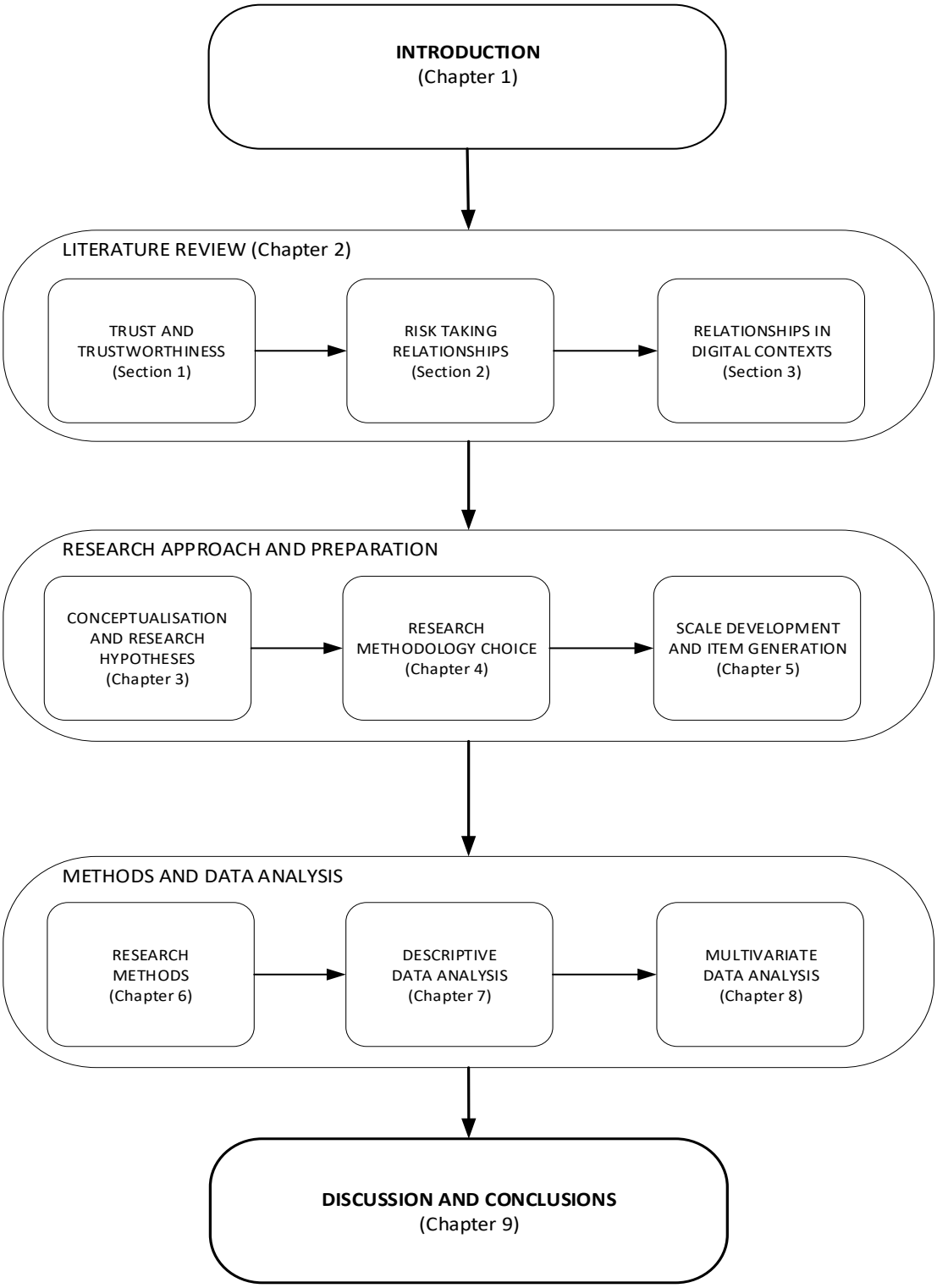


Table 1.1 Thesis Structure

Phase	Research Objective	Purpose	Location
Literature Review	Critical review of relevant theory, literature and prior work.	Critical evaluation of themes and contexts. Frames the academic background of the research problem.	Detailed in Chapter 2 of this thesis divided into 3 sections: • Trust and Trustworthiness • Risk Taking Relationships • Digital Contexts
Conceptual Framework and Research Model	The creation of a framework of concepts and development of theory with which to investigate the research problem.	Provides a conceptual model of the domain of research against which the research findings were evaluated.	Detailed in Chapter 3 of this thesis.
Methodology	Critical analysis of the paradigms of research and their relationship with the reality of the problem space observed.	Methodological choice, justification and selection to guide the interpretation and implementation of the research findings.	Detailed in Chapter 4 of this thesis.
Research Methods	Details the methods of analysis applied to the collected research data.	Rationale and selection of research methods to produce a strategy for fulfilment of the research using the chosen methodology.	Detailed in Chapter 5 of this thesis.
Item Generation and Scale Development	Scaling existing measure items and generating new items where required.	Creation of scaled measurements aligned with the research theme.	Detailed in Chapter 6 of this thesis.
Descriptive Data Analysis	Describe the demographic nature of the sample and the distribution of the data.	Presents the properties of and comparisons between data samples and measurements.	Detailed in Chapter 7 of this thesis.

Phase	Research Objective	Purpose	Location
Multivariate Data Analysis	Logical research model and Hypothesis testing.	Statistically determines whether the findings from the survey support the research model and theory and can inference and generalise.	Detailed in Chapter 8 of this thesis.
Discussion and Conclusion	Presents the research findings and contribution, outlines the limitations of the study and opportunities for further research.	Summarises the research enquiry, assesses how the thesis met the aims and objectives outlined in the introduction.	Detailed in Chapter 9 of this thesis.

The thesis map and structure ensured a flow of narrative from critical analysis of the prior literature, through conceptualisation, approach and preparation of the data collection, detailing the methods and analysis of the data towards the conclusions and recommendations of the enquiry.

1.4 Summary

This introduction to the research enquiry outlines the background, necessity and rationale behind the research problem investigated in this work. It also serves to detail how the research was directed and performed in terms of the questions for which answers were sought, and the objectives that were set to provide answers to those research questions. To provide evidence for the widest applicability of the study, a number of research question contexts were outlined with which to provide stability

and generalisability of the findings. A brief description of the statistical methods that were used to convert the survey data into findings was given, along with the research methodology that was used to interpret those findings.

The key findings from the research are given, and the results interpreted in terms of the potential impact on the development of theory in the investigation areas and in the management of cybersecurity in trust formation.

This introduction describes the audit trail, or chain of custody, of the research effort from prior work and inception of the model through to the extension of theory and the implementation of the findings and their impact on the developing profession of information security management.

2. Literature Review

2.1 Section One: Trust and trustworthiness

The literature review is considered in three sections, trust and trustworthiness; risk-taking relationships; and relationships in digital contexts. This section analyses the academic literature starting with an examination of trust.

2.2 Trust Introduction

Trust is the golden thread that runs through the lives of individuals (Rotter, 1980), it forms an integral part of the organisation of social life (Lewis and Wiegert, 1985) and the functioning of organisations (Dietz and Den Hartog, 2006). Trust intertwines with the fabric of life, mostly unheeded, occasionally becoming frayed or broken, and sometimes, when lost, it can resurface in the most unlikely of situations (Elangovan and Shapiro, 1998). It has survived across the ages as an enabler to individuals and groups and is built into the operation and perpetuation of institutions, governments and information systems (Robinson, Dirks and Ozcelik, 2004). It is the invisible, inconsistent, but persistent presence of trust in society that prompts this enquiry into the relationships between trust and the security of information in blended social and digital environments.

The reality of trusting outcomes are seen in society in everyday exchanges of goods, money, information and ideas between individuals and groups. Trust itself, however, is not physical; it is an abstract latent variable and is used to explain the existence of the interdependencies that enable interactions and exchanges in the physical world. The complex phenomenon of trust appears to play a causal role in the interchange between the psychological processes of individuals and the institutional roles of society, acting as cause, outcome and moderator of exchanges and *"acts as a 'meso' concept that helps to integrate the micro level psychological processes and group dynamics with the macro level institutional arrangements"* (Rousseau et al., 1998:393). Trust spans the divide between individuals and the institutions that facilitate action.

It is a widely held view that trust is a compelling ideal that is important in giving rise to social exchanges as diverse as close personal ties, business relationships and work alliances (Kanter, 1977; Argyle and Little, 1972; Blau, 1964). Given the aforementioned points, it is also necessary to consider what trust is not and to isolate the distinctive core elements of trust. This awareness is used as the basis for a critique of activities that are based on what researchers ascribe to trusting behaviour in physical and online relationships.

In the physical world, the formation of trading relationships is predicated on and facilitated by trust between the parties to an exchange (Whitener et al., 1998), and the use of electronic space to facilitate business interaction similarly relies on interdependence and dependence on others to accomplish personal and

organisational goals (Pinto et al., 1993). Extending the paradigm of trust from physical to online relationships requires first that a generalised definition of trust is put forward and that the types and the outcomes of trust are delineated to give a fuller understanding of how this unseen variable influences and shapes online interactions. This exploration of the foundations of trust is necessary because the cybersecurity domain of research interest is part of a wider landscape of associations and interdependencies that encompass both the physical and online territories. The next section, therefore, deals with a definition of 'What is Trust?' in greater detail to identify what it is and why it is relevant to an understanding of cybersecurity and online relationships.

2.3 What is Trust?

A definition of trust is elusive, precisely because it is purely abstract. It is not seen or observed directly but is felt and is known and recognised as such by those who participate in trusting actions. The presence of trust in relationships is discernible only in retrospect when the outcomes of trusting decisions are apparent, but goes largely unheeded at the time a commitment to trust is made and the outcome of the decision is not yet realised. In this regard it does not differ substantively from other scientific concepts like that of the 'Arrow of Time', where the evidence of its existence is witnessed indirectly in the changing of the seasons and the metrics that count its' passing. Past actions are visible and understandable through the audit trail of history but the future is uncertain and contingent on countless unknown actions and influences. The prevailing consensus view is that trust is a complex and

multidimensional phenomena (Hwang and Lee, 2012; Jones and George 1998; Lewis and Wiegert 1985) and that trust is universal in society, but is not universally applied between situations and parties.

An example of trusting behaviour used by Deutsch (1958) is that of a mother entrusting the care of her child to a babysitter. If her trust is not fulfilled the mother suffers unpleasant consequences, but if the babysitter fulfils her trust then the mother enjoys more advantage than if she had not trusted. In this example, the decision of the mother to trust is a cognitive one, but the assessment of fulfilment of the promise is an evidential one (Wanderer, 2013). The initial trusting decision is based on assessment of the situation, and the wisdom of such decisions can only be retrospectively assessed utilising evidential means.

2.3.1 A Meta-Analysis of Generalised Trust

Due to the latent nature of trust and the multidisciplinary nature of enquiry into the subject it is prudent to synthesize the core elements that constitute trust from previous definitions in published scholarly work. The conceptualisation of trust has presented researchers with difficulties in definition, and not all researchers in the field have chosen to adopt their own definition. The breadth of studies in the field range in both scope and applicability, from broad studies of the generalisability of trust to domain constrained micro definitions.

Many researchers that have formalised trust have framed definitions that reflect the nature of their enquiry into the subject. Many definitions, even of trust as a

generalised concept, contain echoes of the disciplinary language of the viewpoint that has informed the definition, and the imprint of interpersonal, social psychology, economic, sociological, institutional and behavioural science is present in most, if not all of these artefacts. A synopsis of generalised definitions are presented in Table 2.1.

When approaching the subject of generalised trust it is difficult to be agnostic about the genesis of the research journey and to do so would ignore the theoretical contributions, insight, emphasis and nuance that the disciplines have yielded. The definitions of generalised trust contained in Table 2.1 are listed by publication date. These selections represent, of necessity, a subset of the many definitions that are available. Academic work that is included in the meta-analysis is highly cited with a minimum of 700 citations, with the most cited paper (Morgan and Hunt, 1994) having over 24,500 citations. All of the definitions are taken from published books (4) and academic journals (13). Where journal articles have been chosen for a definition both the H5 journal Index score (over 20) and Scimago Journal Rankings (SJR) (over 0.9) have been used to ensure that the work was published in highly ranked peer reviewed journals. The author H Index was also referred to in the selection criteria to give a measure of the academic impact of the author(s) other published works.

Table 2.1 Researcher Definitions of Trust

Author(s)	**Theoretical Contribution**	**Definition**
Deutsch, 1958: 266	Positive Expectation	*"An individual may be said to have trust in the occurrence of an event if he expects its occurrence and his expectations lead to behaviour which he perceives to have greater negative consequences if the expectation is not confirmed than positive motivational experiences if it is confirmed"*
Rotter, 1967: 651	Information communication	*"Interpersonal trust is defined here as an expectancy held by an individual or a group that the word, promise, verbal or written statement of another individual or group can be relied upon."*
Zand, 1972: 230	Trust regulation as a decision	*"Conscious regulation of one's dependence on another that will vary with the task, the situation, and the person"*
Barber, 1983:5	Structure and culture as determinants	*"predominantly as a phenomenon of social structural and cultural variables and not ... as a function of individual personality variables"*
Lewis and Wiegert ,1985 :986	Systemic security	*"The members of that system act according to and are secure in the expected futures constituted by the presence of each other or their symbolic representations"*

Author(s)	**Theoretical Contribution**	**Definition**
Morgan and Hunt, 1994: 23	Reliability and Integrity of trustee	*"*We conceptualize trust as existing when one party has confidence in an exchange partner's reliability and integrity.*"*
Mayer et al., 1995: 712	Willingness to be vulnerable without controls	*"the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party"*
Fukuyama, 1995: 26	Community norms	*"the expectation that arises within a community of regular, honest, and cooperative behaviour, based on commonly shared norms, on part of other members of that community"*
McAllister, 1995: 25	Confidence in the trustee	*"…*the extent to which a person is confident in, and willing to act on the basis of, the words, actions, and decisions of another.*"*
Hosmer, 1995:393	Duty, Volunteerism, Interests	*"Trust is the reliance by one person, group ,or firm upon a voluntarily accepted duty on the part of another person, group, or firm to recognise and protect the rights and interests of all others engaged in a joint endeavour or economic exchange"*
Lewicki and Bunker, 1996: 117	Risk determination and motives	*"a state involving confident positive expectations about another's motives with respect to oneself in situations entailing risk"*

Author(s)	**Theoretical Contribution**	**Definition**
Rousseau 1998: 395	Psychological States	*"Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another"*
Sako, 1998: 388	Reciprocity in the relationship	*"Trust is an expectation held by an agent that its trading partner will behave in a mutually acceptable manner (including an expectation that neither party will exploit the other's vulnerabilities)."*
Sztompka, 1999: 25	Gamble on outcomes	*"A bet about the future contingent actions of others"*
Gambetta 2000: 213	Outcome probability assessment	*"trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action"*
Tomkins 2001: 170	Belief and loyalty	*"The adoption of a belief by one party in a relationship that the other party will not act against his or her interests, where this belief is held without undue doubt or suspicion and in the absence of detailed information about the actions of that other party."*
Barbalet, 2009: 367	Evidential limits	"*Trust, then, is a means of overcoming the absence of evidence, without benefit of the standard of rational proof, which is required to sustain relationships between persons or between a person and a social artefact.*"

Although citations, journal rankings and H indices lend quantitative data as to the authority of published work, the creation of academic facts is a social process (Hyland, 1999) and rankings do not necessarily reflect the impact and contribution of the work to the understanding of the elements of trust. Citation also does not always correspond to agreement with the content of the research and may in some cases citation may indicate active disagreement with the author's viewpoint or merely serve as an acknowledgement of prior work. A subjective assessment of the theoretical contribution of each definition to the understanding of trust has been included in the table to ensure that any synthesised working definition of trust encompasses both contribution to, and peer acceptance of, the importance of the work.

2.3.2 A Generalised Definition of Trust

The need for an enduring generalised structure of trust "*is rooted in the fundamental indeterminacy of social interaction*" (Seligman, 1997:13) and the stability of trust between parties helps to reduce this indeterminacy. To arrive at a 'consensus' view of what this enduring generalised trust resembles entails synthesizing a definition that is comprehensive and grounded, conceptually simple, and applicable across disciplines (McKnight and Chervany, 2001).

The definition of trust makes the following assertions based on the definitions listed in Table 2.1 :

1. Trust is a multiparty enterprise, between trustor(s) and trustee(s).

2. That there is an expectation that trust will produce a greater chance of a positive outcome.
3. Trust involves being willing to be vulnerable, described in the literature in terms of risk, vulnerability or uncertainty.
4. The uncertainty associated with trust is modified by the presence of interpersonal, normative or systemic indicators.
5. Trust is formed irrespective of the ability to monitor or control the other party.

The definition of trust for the purposes of this thesis can be stated as:

"Trust is the confident expectation that a trusting party will engage with other(s) to effect a net positive outcome in situations where risk or uncertainty are present without the ability to monitor or control the other party."

The definition includes the multiparty nature of trust implicit in all of the reviewed academic literature, the expectation of success or confidence on which the trusting action is predicated, and the presence (either implicit or acknowledged) of risk or vulnerability. The manifestation of generalised trust realises the uncertainty attenuating mechanisms and indicators that are also mentioned throughout the academic study of 'What is Trust'. Synthesising an axiomatic definition of generalised trust provides a window into the shared core characteristics of the phenomenon without the idiomatic usefulness offered by assumption constrained models of trust. Then applying insights gained from different disciplinary research into the

characteristics of generalised trust in specific areas helps to confirm the multi-dimensional nature of trust in practice.

The domain studies on the meaning of trust in practice have been utilised to propose types of instantiated trust and how the features of these trust mechanisms elaborate the application of generalised trust. Further study of the dimensions of trust gives a richer understanding of the antecedents, formation processes and consequences of trust in applied situations, the distinguishing features of which are described in the next section.

2.4 Trust Categories

As previously discussed, the predisposing factors involved in the formation of generalised trust have an influence on the instantiated type of trust used in the relationship. Different classes of trust definitions have been proposed. However, one of the problems with trust is that the definition depends upon the disciplinary perspective it is viewed from as *"the psychologist sees trust as a personal trait, the sociologists who see trust as a social structure, and economists who see trust as an economic choice mechanism"* (McKnight, 2000:827). The different, sometimes narrow, constructs used to conceptualise the phenomena reflect the diversity of these views. Conversely, vague prescriptions of generic trust may not be specific enough to address the specificity of the situation.

The following subsections discuss the dominant types of trust (Blanket, Affective, Cognitive, Normative, Encapsulated and Institutional) that can be

differentiated from the generalised trust mechanism. These categories were analysed because they reflect the generalised, non-domain specific characteristics of trust that are inherited by the domain implementations of trusting behaviour.

2.4.1 Blanket trust

In a situation where Party A is the trustor and Party B is the trustee and X is the task or outcome expected from the relationship between A and B, trust can be described as a three-part relationship namely A trusts B to do X (Hardin, 1992). This relationship of blanket trust can be said to exist where the trustor places their trust in a trustee regardless of the situation. This attitude of instinctive boundary-less trust can be traced to the psychosocial development of the individual (Erikson, 1965) where the development of trusting or mistrusting attitudes is developed by the individual during childhood development.

The notion of blanket trust, however, does not take into account the necessity of developing trusting behaviour in different circumstances. A person may only trust another with regard to certain aspects of behaviour, and may distrust them in other areas. Where the trustor has no experience of a trustee, they may not be able to base a judgement on whether they are to be trusted in areas they have no knowledge about (Blois, 1999). The concept of blanket trust is rarely applied because of the existence of different contexts within which the trusting relationship takes place. Trust is not a global feeling of affection but is a result of the regulation of dependence on the other party, and this dependence varies as a function of the tasks, situations, and who the

other party is (Zand, 1972). As contextual factors produce diverse choices in diverse settings (Sunstein, 1996), it stands to reason that parties draw on these contextual influences in drawing boundaries to the trusting relationships between them such that individuals have a number of differentiated trust relationships of varying depth, reach and importance that have been formed as a result of different environmental factors. The application of context is important as being reliant on blanket trust involves delegating all actions to another, with a naivety that can be taken advantage of and which can result in disempowering the trustor. Using boundaries drawn around blanket trust by considering the situational context is one way in which working trust relationships can use the willingness of other parties to cooperate whilst recognising the autonomy of and empowering the individual.

2.4.2 Affective trust

Affective trust occurs where the trustor has a level of confidence that is based on feelings generated by the level of care and concern shown by the trustee and is characterised by the security and perceived strength of the relationship engendered.

Affective trust lends a sense of security through emotional as well as physical security, and is qualitatively different from the 'rational' beliefs associated with other, cognitive, forms of trust (Flores and Solomon, 1998). *"The essence of affective trust is reliance on a partner based on emotions. As emotional connections deepen, trust in a partner may venture beyond that which is justified by available knowledge."* (Johnson and Grayson, 2005: 501). Therefore, affective trust makes assumptions about the

benevolence of the trusted party as *"In trusting them, we trust them to use their discretionary powers competently and non-maliciously, and the latter includes not misleading us about how they have used them."* (Baier, 1986: 240). Affective trust which is engendered by emotional security gives more leeway to the trustee in acting for the trustor than the narrow boundaries of knowledge or responsibility would allow. The trustor relies on the affective signals given by the trustee and the trustee must be moved to care for and commit to the interests of the trustor.

The presence of an affective trust bond lowers the threshold of evidence required for trusting and affective trust plays an important role in the early stages of trusting relationships, where the lack of prior knowledge of a trustee means that there is not enough epistemology on which to base cognitively processed trust decisions. It allows trustors to make subjectively rational choices in situations where ambiguity of outcome would preclude a fuller appreciation of the situation by relying on the individuals' attitudinal stance to guide decisions. In the absence of family ties, affect based trust in organisations has been found to be positively correlated to the levels of citizenship behaviour and frequency of interaction between peers (McAllister, 1995). Affective trust makes trusting behaviour possible through the influence of affective states, moods and emotions on the disposition of the individual, with positive affective states having a positive correlation to trusting behaviour, and negative emotions having a negative influence on such behaviour.

The affective state of the trustor has been shown to be an important influencer on the cognitive processing of trust by determining how trustors feel about their

judgements. The presence of affection allows trusting parties to build cognitive based trust relationships by promoting positive mental states that allow information exchange to take place that can lead to the formation of cognitive trust.

2.4.3 Cognitive trust

Utilising Gambetta's (2000:213) definition that trust *"is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action"*, it is implied that cognitive processes are employed by an agent in the assessment of this probability. Cognitive trust arises from an accumulated knowledge that allows one to make predictions, with a certain level of confidence, that a partner is likely to live up to their trust obligations sourced from other parties or from prior interactions.

Devlin (1992) describes the perceptual acquisition of information, which can be said to consist of two stages. The first stage is the actual act of perceiving, characterised in terms of analogue information. Perception is followed by cognition, the extraction of information in signal form within the mind of the information receiver. Due to the amount of information that is processed, human agents face a loss of information between perception and cognition, meaning that decisions are always based on incomplete information (Miller, 1956). Given this shortcoming in information, trust can become the bridge with which to overcome the knowledge gap (Luhmann, 2000). Cognitive processes use information to build an epistemology to support trust that is based on the individuals' capacity for trust. The capacity to trust

can be influenced both positively or negatively based on attitude and prior experience, which leads individuals to different assessments of the expectation of positive outcomes to the relationship. These decisions are subject to reassessment or revision over time as the epistemological base is built upon. In this regard trust decisions are based on cognition but influenced by attitude, affective trust and information context to provide a subjective rationale.

Cognition based mechanisms suggest that trust has a temporality. The antecedent conditions of trust predate the formation of the trust bond whilst the cognitive trustor is engaged in information gathering (Simon, 1955) and processing that information by cognitive reflection (Frederick, 2005). As Dirks (2000: 1009) noted *"one can argue that expectations about future outcomes in situations of uncertainty are likely to be created by observing past outcomes produced by the party"*. Perception and the posterior processing of these perceptions leads to a cognitive basis for trust and once an initial trust situation has been established and tested, risk is reduced or eliminated.

The parties will be able to continue their relationship through contractual obligation and due diligence mechanisms (Johnson and Grayson, 2005), and these elements of calculativeness in economic trust relationships make the adoption of calculated trust arrangements more widespread in organisations than in social choice settings. It could be debated whether calculative trust constitutes trust at all due to the lack of vulnerability and risk taken by parties, and whether the restrictions of contractual obligation render trusting behaviour unnecessary. In this regard

Williamson (1993) posits that calculative trust is based on the assumptions that a party is aware of the possible range of outcomes and that parties proceed only if net gains can be projected, and then only with the party that offers most net gain. It would appear that calculativeness in practice can only be used as a risk assessment metric with which to measure the lower boundary of trust rather than act as a substitute for it. Nevertheless, even in calculated economic exchanges it is difficult to discern how the initial conditions of the relationship can be determined without some reference being made to affective trust and information sharing between parties who are strangers to one other.

Cognitive and socio-cognitive trust forming mechanisms are a way for agents to assess and evaluate the risk involved in risk taking relationships based on their internal attitude to risk and an evaluation of prior interactions, or 're-cognition' of situations and evaluation of past benefits in the intentions of future action. If cognitive trust is viewed as *"a bet about the future contingent actions of others''* (Sztompka, 1999: 25), then trust can be seen as a way of hedging this bet to improve the odds of a successful outcome for trustors.

Cognitive choices are often made within the context of bounded rationality determined by poor information availability and by the attitude taken by the parties, as taking a bet is contingent upon the kind of bet-taking person the trustors are. Cognitive trust may stray into calculativeness or opportunity where the risk is eliminated or the vulnerability of trustors is known, and as a consequence is rarely insulated from the moderating influences of either normative or affective trust.

2.4.4 Normative trust

The basis of normative trust is predicated on the behaviour of the parties to a trust relationship being guided by the societal norms of behaviour expected within such relationships. In terms of this, Sunstein (1996: 907) commented, *"If a definition is thought necessary, we might, very roughly, understand "norms" to be social attitudes of approval and disapproval, specifying what ought to be done and what ought not to be done"*. Normative trust relies on an agreement as to what constitutes these normative ethics within the society in which the trusting behaviour takes place.

Social relations can be analysed through the building of structures within which the reproduced social practices of agents can take place. The structures allow for similar 'systemic' rules, resources and regulations to exist across varying spans of time and space (Giddens, 1984). The resulting structuration of society provides the continuity of the structures, allowing temporal social systems (like trust) to mutate and reproduce.

The cooperation evident between individuals as a result of the influence of religion, tradition, shared historical experience and other types of cultural interactions has been described as an instantiated informal norm that constitutes social capital, where *"social capital refers to social connections and the attendant norms and trust that facilitate coordination and cooperation for mutual benefit"* (Putnam, 1995: 664). Social capital is manifested as normative trust relationships between individuals, and is related to traditional virtues such as honesty, keeping and making commitments,

social interaction and the reliable performance of duties (Fukuyama, 1995). As such, instantiated normative trust based on social capital is influential in volunteering, advocacy and reciprocal behaviour and can promote accountability and traceability.

Conversely, the elements of normative ethics ensure that effective mechanisms exist with which to ensure compliance and issue sanctions so that the behaviour is regulated. Normative trusting is also context specific and the homogeneity implied by social capital conceals a multiplicity of behaviour patterns that are determined by the encapsulation of the group norms in the behaviour of individuals.

2.4.5 Encapsulated trust

Considering an encapsulated trust viewpoint, the trustor's interests in a positive outcome are 'encapsulated' in the trustor's assessment of the motivations of the trustee. Encapsulated trust is more than the expectations of caring behaviour defined by affective trust, it involves these expectations being grounded in an understanding of the trustees' interests specifically with respect to the trustor, *"Party A will trust party B because Party A's interests are encapsulated in some way by the motivations that they perceive in Party B. The trust bond is formed between Party A and Party B because there is a desire to continue the relationship"* (Hardin, 2002: 4). The author also posits that as the trust relationship continues and becomes richer and more valuable to the partners, the more trusting and trustworthy they are more likely to be in the relationship.

Encapsulated trust involves a cognitive element that recognises the value of an enduring trusting relationship between partners. Encapsulated trust helps to foster confidence and cooperation in the relationship and means that both parties have a stake in contingent events, and from this anticipation trust can create the desired outcome. The notion of trust as a shared endeavour, with contributions to the outcomes from both parties is a strong motivator for goal achievement in environments where there is a power balance between the parties or they both have an interest in the outcomes of trust.

2.4.6 Institutional trust

The role of institutions is to provide and maintain stability and social order of society, and in doing so they provide the foundational conditions for trust in societies. In seeking to achieve this they seek to constrain the freedom of individuals in taking action. Constraint by institutional authority and trust have been found to positively correlate with the provision of stability, protection, and preservation of traditional practices, and negatively with values that emphasize independent thought and action and favour change (Devos et al., 2002).

Institutional trust promotes the engagement of social capital in the trust formation process, and is instrumental in shaping the environment and boundaries of the trusting relationship through the provision of legislative and compliance sanctions. Structural mechanisms are used to increase success through guarantees, contracts, regulation, legal recourse, process or procedures that are in place to give an assurance

of success (Shapiro, 1987). Institutional trust generates systemic trust and trustworthiness by giving guarantees (and rights of recourse) to individuals in dealing with organisations.

On one level a reasonable argument can be made that an institution or an organisation can be considered as a collection of individuals who work towards a common aim. However, the trust bond between the individual and the institution is abstracted so that institutional trust, like interpersonal trust, can be identity-based (Maguire and Phillips, 2008). In viewing organisations as collections of individuals is the notion that people are 'social actors' in fulfilling roles in the organisation and undertake to act in ways that are compatible with their social position (for example, doctors, lawyers, priests, or others who act in public offices), or bound by professional rules of conduct, imposed either by the institution or the profession in which they practice (Sztompka, 2000). Trust in the professions is conferred by their group, the qualifications they hold (and can display for such achievement) and the position that they hold in the social group. Individuals interact with institutions on the 'micro' level when they deal with the practitioners whom they have a trusting relationship, when they act on the 'macro' authority of the institution that has been delegated or has vested authority in them.

Trust between an institution and the individual confers stability, predictableness and structure to the relationship, but conflict can arise when change is required from the trusting relationship. Individuals may view institutions as constraining the capacity of trust to change and produce outcomes, and so may choose to take a mistrustful

stance toward situations where they believe that institutional authority is being wielded.

2.4.7 Trust Categories Summary

The types of trust explored in this section (Affective, Cognitive, Normative, Encapsulated and Institutional) can be seen as subsets of the boundary-less concept of blanket trust, with the ellipsis, exceptions and conditions describing the inclusion and the exclusion of situations not applicable to that context. As such, a rejection of the adoption of blanket trust is required due to the contextual constraints within which it acts. Trust in context (Section 3.2.9) is an emergent of the circumstances of attitude, expectation and risk. In differing situations the structures in place are used as a prism through which the specialised manifest types of trust are refracted.

The variation in types by which latent generalised trust is instantiated lend weight to the viewpoint that trust is a multidimensional variable, and as such it represents an abstract in which antecedent conditions and contextual factors interplay and influence the behaviours (and outcomes) of the affairs of individuals and organisations. The emergence of trust from its antecedents results in the particular consequences that are symptomatic of the presence of trust. Latent trust and context predicate the manifestation of trust that is observable in the characteristics of trusting relationships. These observations, or outcomes, of the relationship are explored in the next section.

2.5 Outcomes of Trust

Trust made manifest in behaviour between parties has important consequent effects on the nature of relationships. This, in turn, is highly influential in future behaviours and attitudes adopted by both parties to the trusting relationship. The consequential behaviour of trusting decisions can be seen to define the externally visible characteristics of trust. The symptoms of trust are shaped by the type of trusting relationship that is formed between the parties and which help to mobilise the risk reduction and expected outcome strategies stemming from the decision to trust. Therefore it is necessary to examine the outcomes and unique characteristics of trust relationships in the next sub sections.

2.5.1 Co-operation

Cooperation in trusting relationships involves an encapsulated commitment to the interests of the other party and indicates a motivation to work towards a common positive outcome for both parties, even where doing so is not necessarily in the short-term interests of that party. *"Cooperation is an act that increases the welfare of the other(s) at some opportunity cost where the former is greater than the latter. The forgone opportunity cost (potential gains from defection) is the hallmark of cooperation"* (Yamagishi et al., 2005:277). Cooperation and tact allow trust to be sustained and maintained without unnecessary friction between the parties and allows considered judgements to be applied and so allows the permissible boundaries of the trusting relationship to be tested. Cooperation in trusting relationships is aided

by the presence of social capital between the parties and the manifestations of shared endeavour and encapsulated interest that the presence of social capital facilitates.

Yamagishi and Yamagishi (1994) highlight cultural differences in trust according to the bias that is placed on where incomplete information is available and looks at the incentives for parties in a trust relationship to act cooperatively to reduce the information gap. The authors note that commitment to a trust relationship can become a liability if the opportunity costs increase. Work to generalise the findings of Yamagishi's 'Emancipation theory of trust' by Georghiu et al., (2009) confirmed a significant relationship between the social trust shown in different nationalities due to the relative weights of individual and collective mental programming (Hofstede, 1980), regardless of the political history or ethnic composition of each country. The emancipation theory predicts that increased opportunity costs can lead to a competitive situation for resources that can result in new uncertainties and opportunities.

Although sometimes viewed as a negative attribute, competition forms the corollary to cooperation and brings with it its own benefits and drawbacks (Fehr and Schmidt, 1999). Whereas cooperation, faith and confidence are often used synonymously with trust and competition, resistance and defensiveness are used interchangeably with suspicion (Kee and Knox, 1970). However, competition and opportunism, the *"self-interest seeking with guile"* (Williamson, 1993: 458) can be shown to increase productivity and promote positive change by acknowledging

previous knowledge as well as having negative consequences including trust breaking and information withholding.

Cooperation can happen in the absence of trust. Without trust, cooperation is reduced to mere behavioural compliance, and the imposition of institutional or social controls may be sufficient to ensure that sufficient cooperation is given. Cooperation without trust can lead to less satisfactory outcomes due to the lack of communication between parties. However, trust is contingent upon the cooperation between trusting parties, and without which would lead to a loss of confidence, an increase in risk and ultimately a loss of trust.

2.5.2 Communication Quality

Cooperation also involves bi-directional communication between parties, and if communication is a form of cognition by proxy (Origgi, 2004), then increased cooperation promotes the amount of cognitive trust present in a relationship.

The presence of cooperative communication in the relationship involves elements of give and take, and the exercise of openness, tact and forgiveness between parties serves as a negotiation and boundary setting mechanism. Communication and information sharing decreases the amount of incomplete information in a relationship and can lead to an increase in the alternatives open to the parties to achieve outcomes. It allows trust-offering to be offered without hostility, and allows the parties to recover their position and be forgiven without loss of face when misunderstandings or incorrect information is passed between parties (Baier, 1986).

2.5.3 Mistrust

Although trust and mistrust can be said to form a continuum mistrust does not always necessitate a lack of cooperative behaviour. There are situations where mistrust is the driver of the trustor-trustee relationship. Mistrustful actions are the result of more guarded behaviour and are derived from the attitudinal stance adopted by the parties.

A mistrustful stance can be instantiated as mistrust as a result of the personal development of the individual; where a power asymmetry exists; or where previous contextual conflict has led to a guarded or vigilant approach to trusting. Whereas trusting partners trust, mistrustful parties will seek to trust but also to verify that trust. Mistrust situations are also able to deliver mutually beneficial outcomes but do so by using different mechanisms and functions to achieve those outcomes. *"Mistrust is a cautious attitude that propels citizens to maintain a watchful eye on the political and social happenings within their communities. Moreover, mistrust depends on trust"* (Lenard, 2008: 312).

Where vulnerability is present in a relationship the dynamics of relative power need to be considered. As the vulnerability of the trustor is one of the antecedents of trust, the relative power of the trusted party may amplify the feelings of powerlessness in the trustor, and so contribute to feelings of insecurity and mistrust (Baier, 1986). The boundaries of trust, mistrust and simply not knowing where the boundaries are in situations can lead to grey areas and conflict in relationships. This

can lead to the vigilant trust with verification where both sides to a relationship seek to not rely on trust by imposing controls and monitoring each other. In situations where trusting parties used to trust but no longer cooperate, or there was a perceived betrayal, the epistemology of trust and its authority endures in the functions employed in the mistrustful relationship.

2.5.4 Betrayal

Parties may seek to make alternative trust arrangements that involve trust being broken. Trust breaking may be precipitated where the situation demanded by the antecedents of trust have changed or trust may breakdown due to the expectations of the trust bond not being met. There are several dimensions where the trusting expectations may fail, and these can be classified as *"the continuity of the natural and the moral order, the technical competence of actors in roles, and the fiduciary obligations of actors, their duty and their motives to place the interests of others before their own."* Luhmann, 2000:95).

Where trust is breached, it is seen as a way to break the cognitive inertia that is used to maintain committed relations in stable situations. Inertia promotes the preservation of trust by protecting reputation in the face of challenges to integrity and viability (Good, 2000). This can lead to a confirmation bias that can preserve relationships with negative internal features or negative externalities. Breaking trust involves changing the relationship between trustor and trustee and the contracts and

obligations this entails. Trust breaking can also involve the destruction of trusting bonds with other parties that are aligned with the other party.

Deeper than the imposition of contract, trust entails other attachments. There are parallels with Sztompka's (1999) portrayal of former communist East Europeans joining a 'European home' rather than a 'European house' with all the soft trappings of intimacies, loyalties and attachments that this entails. This reflects the deep psychological effects of making and breaking these types of affective and historical bonds. Breaking strong affective bonds can lead to a sense of vulnerability and violation in trustors and when a trust violation takes place individuals seek to make sense of the shock of negative events by using cognitive processes. They seek the responsible party and assess the cause of betrayal and attribute the responsibility to either a party or the situation, and the frequency of previous occurrences (Elangovan, 2007). Betrayal may lead to a revenge situation where retribution is sought against the perceived betrayer to 'get even'. However, as Bies et al., (1996:247) posit trust breaking can also be a *"potent motivator for change or cooperation and a powerful constraint against power abuse"* Breaking the inertia of the situation by trust busting can be a creative destruction, as the trusting party becomes aware of the risks that they were taking as part of the relationship.

In some cases trusted parties may delegate actions to others to fulfil and trustors may not always trust the delegated trust relationship. Research into the place of strong and weak delegation of trusting authority to other agents to fulfil trust revealed that the trust bond between the two parties is not always transitive, and that

delegation of trust is not always beneficial to the relationship (Castelfranchi and Falcone, 1998). Although it has been argued that betrayal is not a failure of trust but a failure of trustworthiness (Hardin, 2002), multiple delegated contexts require that the trustor not only places their trust in the trusted party, but also has trust for all other parties that the trust relationship operates through.

Once a trusted partner has betrayed the trust they are subsequently trusted less, if at all, as the history of perceived betrayal can undermine the relationship. In situations where the risk taking relationship breaks down the failure of trust may act as a catalyst for change. Betrayal of affective trust can result in other externalities, including revenge taking, competitive behaviour and the destruction and renewal of other peripheral trusted relationships.

2.5.5 Reciprocity

Rooted in Blau's (1964) Social Exchange Theory, many trust relationships display a mutual aspect to the trust relationship, a reciprocal arrangement that facilitates social exchanges. Social exchange can arise as a result of either reciprocal exchange or by negotiated exchange (exchange by contract). Yamagishi and Yamagishi (1994) make a distinction between the affective trusting nature of the bi-directionality of reciprocal behaviour and the 'assurance' afforded by negotiated exchange, underpinned by terms, conditions and the constraints imposed by contracts.

Reciprocal exchange involves being reliant upon the trusting behaviour of partners with the attendant risk as, *"Since there is no way to assure an appropriate*

return for a favour, social exchange requires trusting others to discharge their obligations" Blau, (1964: 93-94). This discharge of obligations and assistance indicates the role of social capital and the level of trust, and is employed within nations to promote co-operation (Fukuyama 1995; 2001). It enables individuals to leverage their trust networks to interact with other groups to attain selfish and group outcomes. The 'Radius of Trust' model allows groups to overlap, and is characterised by strong internal ties and weak associative ties between groups. The latent variable of social capital fosters reciprocity as a way of facilitating associations and reducing the friction associated with co-operating in public life. Thus, social networks can exert positive or negative influences and externalities to the wider society through social capital instantiated in elevated trust levels.

Research into the membership of professional associations has also shown that trust acts as a significant mediator in professional relationships and that members of a professional association are more willing to advocate for the association and its' members (Huang and Chen, 2016). Building reciprocal exchange relationships can enhance the motivation of members to participate in reciprocity, and create the motivation to advocate for the role of others.

Although trust may include reciprocal social exchange it is not dependent upon it. Where mistrust is the driver of behaviour in situations and the bi-directionality of the trust relationship is not demonstrated or needed, or where a power asymmetry precludes the formation of a mutual trust bond then *"adaptive and collaborative behaviours are expected to result in mutual gains, these gains may not be fairly shared*

among the partners" (Nyaga et al., 2013: 47). Experimental research undertaken to evaluate the reciprocity of trust behaviour in reciprocal exchange systems compared to negotiated exchange found that, *"reciprocal exchange produces stronger trust and affective commitment than negotiated exchange, and that behaviours signalling the partner's trustworthiness have greater impact on trust in reciprocal exchange"* (Molm et al., 2000: 1396). When it comes to reciprocity in a trusting relationship the influence of affective generosity is more reliable than ensuring compliance by negotiation.

2.5.6 Predictability

The predictability or reliability of a party is an indicator of commitment to trusting and it provides the support on which trusting actions can be based. Being able to count on others allows individuals to concentrate on realising the outcomes of the trusting relationship without having to check up on the details of how this is being done. Predictability delivers a confidence that the actions of trusting parties will facilitate the expectations of the relationship through prior experience.

Although the terms trust and reliance are sometimes used interchangeably a distinction can be made whereby trust encompasses more than the simple reliance that a party will be more than just dependable as *"what distinguishes trust from reliance is the expectation that the other party may take initiatives (or exercise discretion) to utilize new opportunities to our advantage, over and above what was either explicitly or implicitly promised"* (Blois, 1999: 199). Trusting relationships utilise goodwill over and above the dependable habits of the trustee. The stance taken by

(Baier, 1986) makes a distinction between trust and reliance by noting that trust can be betrayed, but that a failure of reliance can only be disappointed. This point has relevance in electronic systems where trust may only be reliance on the machines that deliver the trustees part of the contract.

To be meaningful, trusting relationships must go beyond the predictability of a party, and using predictability as risk or uncertainty reduction will only take a trusting relationship so far and *"to equate the two is to suggest that a party who can be expected to consistently ignore the needs of others and act in a self-interested fashion is therefore trusted, because the party is predictable. What is missing from such an approach is the willingness to take a risk in the relationship and to be vulnerable. "* (Mayer et al., 1995:714).

To fully realise the benefits of risk taking in a relationship the parties strategic interests' may be best served when there is flexibility and adaptability of cooperation combined with predictability of action which increases the variety of situations and an acceptance of vulnerability with which parties can adapt.

2.5.7 Trust Outcomes Summary

The presence of trust in relationships is discernible from the outcomes that result from the interaction. Important benefits to trusting relationships come in the form of co-operation, reciprocated behaviour (either immediate or delayed), and in the predictability of the actions of the exchange partner. Short of trust, mistrusting relationships are a form of co-operation that relies on knowing the boundaries of

which areas cannot be trusted and taking steps to guard against or verify the actions of the other party. The benefits of trusting come with the potential drawback of betrayal, where perceived contract violation can result in relationship breakdown and reprisals between parties. Therefore, an appreciation of the balance between benefits and drawbacks is necessary when entering into a risk taking, trusting relationship with another party.

2.6 Trust Conclusion

Trust is robust and distinguishable as a phenomenon and the antecedents and outcomes of trusting behaviour are consistent across situations. Trust displays a unity in latency but diversity in manifestation and is displayed regardless of the interpretation of its mode of formation.

A synthesised definition of trust based on published academic definitions was used to derive a consensus definition that was used throughout this work. This latent variable is instantiated within situations determined by the antecedent conditions and results in differing types of trust that use these antecedents as preconditions for trust formation. Once the bond between trusting parties is formed, the resultant relationship is evaluated in retrospect with reference to the desired risk reduction and fulfilment of expected outcomes with respect to the situation.

This section of the literature review has introduced and analysed the core concepts of latent trust, the types of trust that can be discerned, and the outcomes of the presence of trust in relationships. In doing so, it has framed trust as an attribute

of the party that has confidence in, or places faith in another party. However, for this confidence to be fulfilled it is also necessary to research the characteristics of the trusted party.

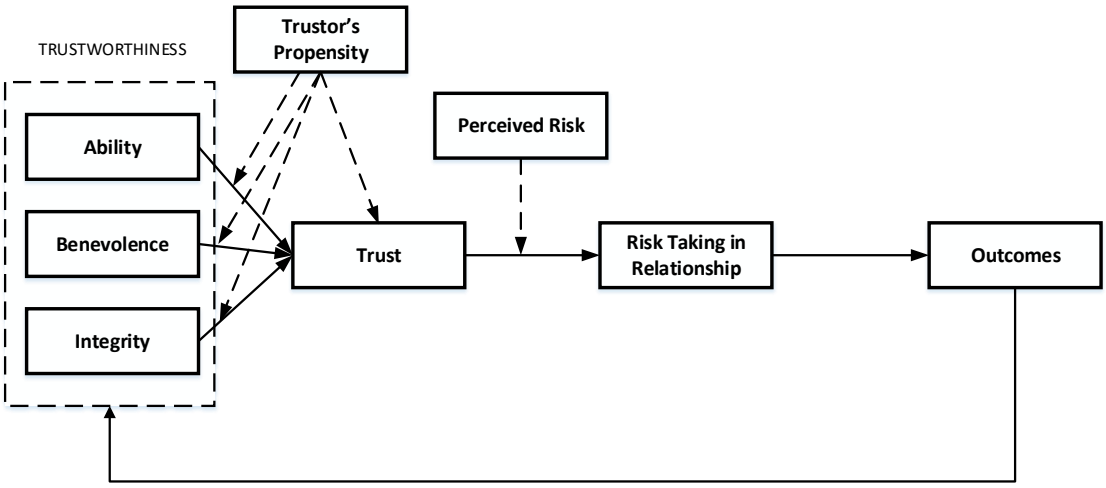
The extent to which trust relationships can develop to encompass risk taking and growth is influenced by the perceived trustworthiness of a trusted party in eliciting the trust of the trustor. Trustworthiness is also a latent variable embedded into social and technological systems where multiple factors influence the decision by the trusting parties to engage in a risk taking relationship. An examination of trustworthiness is given in the next section to understand why it is important in setting the contextual boundaries within which trusting, risk taking, relationships occur.

2.7 Trustworthiness Introduction

A trustworthy partner is one that is worthy of the trust of others and thus trustworthiness is an indicator of the amount of trust a party can command. The previous section analysed the literature relating to the definition and nature of trust. The next section extends this analysis to include a consideration of trustworthiness. Trustworthiness has been described as the *'mirror image'* (Lauer and Deng, 2007) or complement of trust, and empirical research suggests that trust and trustworthiness are separate constructs that have a common association (Evans et al., 2008). A review of the attributes that project trustworthiness is given so that the common association of how trustworthiness elicits trust can be understood.

As a separate upstream construct with its own properties trustworthiness can be seen as the key mediator of the relationship between the antecedents of trust and levels of trust that exist in a risk taking relationship (Sekhon et al., 2014). This chapter uses a starting point of the Mayer et al., (1995) definition of the trustworthiness dimensions of Ability, Integrity and Benevolence, these components are critically analysed to ascertain how they influence the elicitation of trust.

Figure 2-1 Mayer et al. Model of Organisational Trust



2.8 Ability Measures

The expectation of a positive outcome to the actions carried out within trusting relationships has long been a major and persistent feature of the study of trust (Deutsch 1958; Lewis and Wiegert 1985; Mayer et al 1995; Rousseau et al., 1998; Yamagishi and Yamagishi, 1994). Expectation of positive association has been demonstrated in the definition of generalised trust given in **Section 2.2.2**. It is the expectation of positive outcomes that precipitates trusting action, and an assessment

of what constitutes trustworthiness from a trustee is dependent upon the party possessing, or being perceived to possess, both the competence to fulfil and motivation to act to obtain positive outcomes.

2.8.1 Competence

Showing competence in a domain gives a trustor confidence that the outcomes have an increased chance of being met. For a trustee to possess competence, it is necessary for them to display a skill, an expertise or to exert influence within that area. Competence has been variously referred to as ability (Mayer et al., 1995), competence (Barber, 1983) or expertise (Johnson et al., 2005) in the literature. The inclusion of domain is critical to assessing the trustworthiness of a party, as one party may not be competent across all aspects of an expectation, especially where a wide range of different outcomes are anticipated (Zand, 1972; Blois, 1999).

The outcomes of expectation are based on the trusted partners' ability to give confidence to trustors that they possess the ability, competence and characteristics to have influence within that context (Mayer et al., 1995). Prior knowledge of the trustee is required with which to make an assessment of their competence and credibility with respect to the matter at hand. Competence or ability is demonstrated to trustors through communicating prior relevant experience, certifications or accreditations that attest to their expertise. Competence is gained in previous tasks, and the successful outcomes of those tasks are conveyed through the positive (or negative) reputation that a trustee has earned with those previous engagements.

Competence engenders a feeling of confidence within trustors that the expectations can be met, but this must be accompanied by the motivation to act.

2.8.2 Trustee Motivation

The motivation to deliver on commitments made by trustees acknowledges that, although a party may be competent and may have the ability to perform some task, they are not compelled to put this commitment into action as *"Trustworthiness is judged, not merely on the basis of claiming commitments to be trustworthy, but in being able to fulfil the trust placed in them by others."* (Hardin, 2002: 28).

The driver of the motivation to fulfil by undertaking action is a consequence of the type of trust that exists between the parties. Motive is derived from the affective, cognitive, normative, encapsulated, or institutional trust relationship (**Section 2.3**) that the parties are engaged in and the commitment to acting on this motivation by action is mobilised by normative influences and institutional controls. Trustees are committed to action since this involves more than just saying they will do something, commitment is manifested by knowing of the trustees' disposition; their available options and their consequences; their ability; and that they would choose to do with it (Dasgupta, 2000). Motivation is the dimension of trustworthiness that precipitates commitment and action from trustees to realise the expected outcomes of the trusting relationship.

2.8.3 Ability Summary

What marks out the fundamental difference between reliance and trust is that reliance is based on proven capability, whereas trust is dependent on the shared commitment of the parties (Blois, 1999). Ability, as a combination of both competence and motivation to fulfil tasks or actions, is a facet of trustworthiness that mirrors the expectation and confidence of the trusting party. The next sub section analyses the role that another factor, stability, takes in the fulfilment of expectations of trustee behaviour.

2.9 Stability Indicators

Vulnerability is inherent in the preconditions of trust (Mayer et al., 1995), and the purpose of entering a trusting relationship is, in part, to reduce the risk, uncertainty and perceived threats that are felt by the trustor. In being willing to be vulnerable a party will seek to trust in some other party that is perceived to be to a greater or lesser extent reliable, dependable and predictable. Trusting parties receive some sense of security that the threats posed by the uncertain or risky situation can be managed. Although there is no risk involved in the willingness to be vulnerable, but is inherent in the behavioural manifestation of this willingness (Mayer et al., 1995).

Trustworthiness as a stability indicator introduces the capabilities of trustees to provide a stable environment from within which trustors can draw on whilst focusing on the future outcomes of the relationship. Stability in a trustee is assessed cognitively, although trustors may choose to trade the objectivity and reliability this

affords for a measure of flexibility (Guba, 1981). The dimensions of stability include integrity and assurance that influence the perception of predictability, complexity reduction, and trustworthy behaviours in a party.

2.9.1 Integrity

Integrity is related to the perception that the trustor observers a set of principles or values that the trustor finds acceptable (Mayer et al., 1995). The integrity of a trustee is their guiding moral compass and is evidenced in the way in which their beliefs were made manifest through past behaviour and track record. As such, integrity is a feature of the character of the trustee. As noted by McKnight and Chervaney (2001:49) that *"Integrity means that one believes that the other party makes good faith agreements, tells the truth, acts ethically, and fulfils promises"* .

As future outcomes are not guaranteed trustees who were unable to deliver an expected outcome because they 'tried but couldn't' deliver are seen as more worthy of forgiveness than trustees who failed an outcome because they 'tried but didn't' do the right thing (Elangovan, 2007). This suggests that the openness and honesty with which trustees signal their values and efforts on behalf of the trustor is one of the outward signs of integrity. Therefore, integrity yields a measure of reliability, consistency or predictability in uncertain situations and knowing that a trustee will act with integrity defined by their guiding principles instils a feeling of confidence in the trustor.

2.9.2 Assurance

Assurance provides the institutional ground rules by which the integrity and stability of governance is applied to uncertain environments within which the trust relationships operate. Formalising trust relationships by contract or promise is a feature of many personal and organisational interactions. Providing assurance by contract can be seen as an artificially contrived and secured case of mutual trust (Baier, 1986). The normalising and normative effects of contract on trusting relationships can act as an enforcer of rules to deter opportunistic action and ensure promise fulfilment. Assurance acts as a form of institutional integrity that performs an external motivation for participants to play by rules, and affords security by enforcing them by deterrence.

Institutions play a role in enhancing the external trustworthiness credentials of affiliated parties and provide structural assurance and situational normality (McKnight and Chervany, 2001) that allows trustors to gain a sense of security. It enables the monitoring and assessment of the actors who fulfil social roles and the fulfilment of contract duty formalises outcome expectation. The deterrence effect of institutional assurances help to reduce trustor vulnerability. However, institutional trust cannot always be flexible to cope with unknown future outcomes and scholars have discussed to what extent stable expectations and the presence of contract can provide trust over and above reliability (Rousseau et al., 1998). It is also the case that in trusting institutions individuals may be motivated by feelings of doubt, such as when trusting the discretion of police or security agencies. In such cases it is the absence of the institution and not its presence which would destabilize trust (Baier, 1986).

Institutional control measures promote the stability of trustworthiness through contract and regulation. These measures deter opportunism by moderating the actions of individuals and providing assurances of consistent behaviour from trustee organisations.

2.9.3 Stability Summary

Stability enhances trustworthiness through the provision of mechanisms to promote predictability to reduce risk, by providing complexity reduction and ability sharing, showing integrity through shared values, and providing the reliance of contract and structural assurance.

The stability facets of trustworthiness demonstrate a future focused commitment to trust relationships by providing a measure of predictability to reassure trustors. The perception of stability and reliance affords a longitudinal umbrella of care and benevolence that is examined in the next sub section.

2.10 Benevolent Behaviours

A trustee must be able to demonstrate goodwill towards the aspirations of the trustor to form a relationship. In this respect the perceived presence of goodwill and the participant stance perform the same function of elevating the status of trust above reliance (Wright and Enhert, 2010). By communicating a trustworthy attitude through a benevolent disposition this allows the trustor to feel cared for and about. Through creating a relationship in which repeated interactions can deepen the trust bond, the

attitude oriented measures of trustworthiness complement the cognitive rationality aspects of trust in a relationship by providing a feeling of identification between parties.

2.10.1 Benevolence

The benevolence of a trustee is the extent to which they have the trustors' interests in mind in the relationship, and it encompasses more than a simple commitment to not lying or merely fulfilling the reliability criteria for such a relationship. As *"benevolence is the extent to which a trustee is believed to want to do good to the trustor, aside from an egocentric profit motive."* (Mayer et al., 1995: 718) this suggests that benevolence is based on forming a rapport between the parties in which the trustors' interests are placed above those of the trustee, even when it is inconvenient for the trustor.

Benevolence also reflects the trust placed in the trustee by sharing some of the goodwill dividends of trust with the trustor and a benevolent trustee will seek to act in the interests of the trustor by not acting opportunistically. Benevolence is an attribute of the relationship between the two parties and is shown by trustees through the provision of security, showing flexibility, tact and discretion in the exercising of trust in the relationship. The benevolent aspects of trustworthiness are derived from the caring attitude that is shown by the trustee, and is a manifested in the affective relationship between partners. In showing an attitude of benevolence trustees take a longer-term view of the value of a relationship where delayed or developed

reciprocity is a characteristic (Rousseau et al., 1998), rather than viewing it as a wholly cognitive or calculative transaction.

2.10.2 Disposition

The disposition of a trustee is a reflection of the trustors' participant stance and is demonstrated in their orientation toward one another. The participant stance is a manifestation of the attitude that is adopted by the trustor and places personal limitations on the boundaries of the possible and not possible for individuals (Holton, 1994). By showing a trustworthy disposition trustees signal their cooperative intentions towards the trustor and helps the trustor to identify with the trustee.

As noted by Deutsch (1958:271), *"In experimental conditions, a co-operative orientation primarily leads the individual to make a co-operative choice and results in mutual gain, while a competitive orientation primarily leads the individual to make a non-cooperative choice that results in mutual loss"*. A disposition towards co-operative choice produces both trusting and trustworthy behavioural outcomes. Disposition, like integrity, is a way of manifesting the willingness of a trustee to participate in a mutually beneficial relationship.

It can be self-referential in that it is first necessary to trust in order to be trusted, and in displaying this type of behaviour trustees can show their faith in the other party. In displaying a helpful, co-operative disposition towards the trustor a trustee is helping to strengthen affective trust.

2.10.3 Benevolence Summary

Benevolence and a disposition of care above the immediate needs of the trustor on the part of the trustee organisation demonstrates a longer-term commitment to the welfare of the relationship. As well as catering to the cognitive and calculative evaluation of trust, benevolence and disposition elicit affective trust bonding.

The expression and communication of the ability, stability and benevolence of a trustee are ways to cultivate the expectant confidence of trustors. These qualities are communicated to other parties, examined in the next section.

2.11 Communicating Trustworthiness

Trust is an endogenous attribute of the relationship between parties, whilst trustworthiness can be viewed as an exogenous attribute of those parties (Barney and Hansen, 1994). It is therefore necessary for a trusted party to be able to communicate their trustworthiness externally to potential trusting parties. By showing the dimensions of trustworthiness a party is able to communicate that they are capable of reducing a trustor's risk and vulnerability. A trustworthy partner has to show that the trust commitment will motivate an intention to relevant actions in the future to meet the expectation of outcome for the trustor.

In communicating to a potential trustor, the trustee relies on making 'process cues' that aid the decision process to elicit behavioural responses. This allows

potential trustors to assess the trustworthiness of exchange partners through the use of heuristics and network ties (Djupe and Calfano, 2009; Wang, Beatty and Foxx, 2004; Granovetter, 1973). Although it is not possible to generate trust directly *"Commonly, the best device for creating trust is to create and support trustworthiness"* (Hardin, 2002:28). So creating trustworthiness means being able to communicate with sincerity the characteristics that make a party trustworthy, as trust only provides a significance when instantiated through the relationships between parties (Flores and Solomon, 1998; Blois, 1999). A trustee is not only being trusted to deliver the expected outcome with respect to competent risk reduction and reliability, but to deliver it with an élan that inspires confidence in the trustor.

Trustworthiness is communicated by the trustee prior to the trusting relationship, and *"Typically, one party, the sender, must choose whether and how to communicate (or signal) that information, and the other party, the receiver, must choose how to interpret the signal."* (Connolley et al., 2011:39). Trustworthiness prompts are used to communicate the competence, stability and benevolence credentials of one party to another. This information communication requires that there are two parties involved, an information source and an information recipient. The trustworthy attributes of a trustee are defined by the perceptions of the trustor; their assessment of the antecedents; the trust forming context; and by processing the trustworthiness signals that are received (Nurse et al., 2011). Trustors utilise the perception, assessment, context and signals of trustworthiness to give rise to a degree of belief in the trustee and can, with reasonable probability, infer that the relationship

will be a trusting one. Conversely, in providing the trustworthiness signals potential trustees are able to influence these same perceptions, assessment and context to induce the belief that a trusting relationship is possible between the parties.

2.11.1 Reputation

Reputation is the exogenous component of trustworthiness and has been defined as *"The overall evaluation of a company over time based on direct experience and any other form of communication and symbolism that provides information about a firm"* (Gotsi and Wilson, 2001:29). Reputation conveys that the members of the system act according to and are secure in the expected futures constituted by the presence of each other or their symbolic representations (Lewis and Wiegert, 1985). Cognitive shortcuts like product brands are used by organisations to create cultural symbols that signal that individuals share the same tastes and values (Kay, 2006). These symbols are used to 'anchor' the trustor in an area where the familiar and unfamiliar are signposted and the interaction between individuals and organisations provides stability and complexity dampening effects.

The most direct source of reputation is that of experience. Digital environments make direct experience less common, and the reputation of organisations is often made via electronic recommendation and communication systems (Jøsang et al., 2007). The communication between parties does not always constitute a dyad between the trustor and trustee, as trustors often rely on other, possibly multiple or conflicting sources, of information to verify the credentials of a trustee (Liu, 2009).

The signals passed to trustors about trustworthiness are not passed through the same medium which transactions are conducted (Gerck et al., 2001), and the presence and memory of completed historical transactions also contributes to the trust formation process (Yamagishi et al., 2005). Demonstrating transactional trustworthiness allows trustors to build a trusted relationship context within which the purposes of the relationship are realised, as *"Claims to trustworthiness are part of the context in which trust is given, not its' basis"* (Barbalet, 2009:372).

2.11.2 Predictability

Predictability in a given situation means that trustors can have belief in the reliability and behaviour of the trusted party in exchange situations. This belief can be reinforced with successive interactions, thus providing a consistency of action that trustors will act in a certain way. The predictability of a partner's behaviour is *"influenced by a host of factors including such basic elements as the consistency of recurrent behaviour and the stability of the social environment."* (Rempel, Holmes, and Zanna, 1985:96). Stable prior actions aids the projection of anticipated future behaviour to be predicted.

Trustworthiness is displayed through the history of previous interactions with a party as well as being dependent upon the reward structures that are in place (Rotter, 1980). As such, it can be influenced by the completeness of information regarding a party and the regulation of the environment to influence behaviour reward. Predictability can be manifested in consistently good or bad behaviour, and trustors

rely on previous knowledge of a party to assess the trustworthiness of a party in respect to the trusting situation.

In choosing to interact with predicable partners, trustors can reduce behavioural and conduct risk and the controls necessary to monitor the relationship. Providing predictable outcomes fosters trust by reducing both the need and the costs associated in monitoring the relationship.

2.11.3 Complexity Reduction

Trust can be viewed as a mechanism to increase the 'requisite variety' required of a party to interact in the world by increasing the complexity of situations with which they can interact (Ashby and Goldstein, 2011). Although the assertion that trust *"reduces social complexity by going beyond available information and generalising expectations of behaviour in that it replaces missing information with an internally guaranteed certainty"* (Luhmann, 2018: 93) may be overstated it is nonetheless used as a form of environmental complexity reduction. Therefore, part of being trustworthy means that trustors can confidently delegate trusted actions to others who they deem suitable to carry out the duty. In such cases, where the trustor does not need to know about or monitor the task at hand they are freed up to concentrate on other matters.

In managing uncertainty trust can be used as a 'bridge' (Luhmann, 2018), not only between the interpersonal and systemic level, but also between the actions of the past and expected future outcomes. The trust relationship acts as a complexity

attenuator when applied to situations but also acts as a capability amplifier of the parties involved to absorb environmental variation.

2.11.4 Communicating Summary

Trustworthiness is a variable that needs to be communicated to potential trustors. Reputation is the mechanism by which trustors are able to evaluate the latent trustworthiness of trustees in terms of their competence, ability and benevolence characteristics. Reputation is not evaluated entirely by communication, history, symbols or by trustees self-certifying their credentials, but also by other parties vouching for or advocating their trustworthiness. Indeed, the prevalence of online business means that users have to rely more frequently on transactions with people that they do not know.

The reputation of an organisation must be communicated in a predictable fashion to reassure trusting parties that they are capable of reducing risk and minimising the complexity of situations requiring trust.

2.12 Trust and Trustworthiness Conclusion

By critically analysing the literature on the two latent constructs of trust and trustworthiness this section used a meta-analysis of trust to derive a generalised definition of what trust is. This generalised definition was further refined to include a taxonomy of different trust categories inherited from the generic trust definition. The symptoms or consequences of trust in praxis were also explored to understand how

the linked construct of trustworthiness can be inferred to complement the confident expectations of trust.

The critical analysis of trustworthiness was accomplished by first examining the component dimensions of Ability, Integrity (stability) and Benevolence to determine how these antecedent factors in trustworthiness can be communicated to potential trustors to elicit relationship formation. These variables, based on the tripartite view of trustworthiness taken by Mayer et al. (1995) were then analysed alongside their role in producing reputation, predictability and complexity reduction in terms of how they influence the signals of trustworthy behaviour.

Trustors and trustees construct different viewpoints of a trusting situation prior to a relationship. Trustors will be inclined to view a trust relationship within the constraints of vulnerability, perceived control, expected outcome and attitude. Trustees seek to complement or conjugate this viewpoint within a cooperative situation. However, given that trust involves showing vulnerability under conditions of risk without the need to monitor, the resultant trust would be blanket trust or blind faith placed in a trustee, with no controls in place. As blanket trust in contexts is not desirable, the necessity for controls is required to reach a situation in which risk is dampened, controls are implemented, expectation is met and attitude is catered for.

The overlap of the differing, related constructs of trust and trustworthiness delineates the boundaries and possibilities of a risk taking relationship between the parties. It is therefore necessary to examine in the next section how the context for

trust and trusting relationships is framed and instantiated, and how different factors provide the conditions for the genesis of trusting, risk taking relationships.

2.13 Section Two: Risk Taking Relationships

The examination of trust and trustworthiness in the previous section set the background for how the trusting, risk taking relationship is formed in social environments where there is generally face-to-face communication between the parties to the relationship. Adopting a decision analysis approach to relationship formation process adds to the previous chapter because a number of important issues are dealt with. These include how the latent variables of trust and trustworthiness become actualised in relationships through the factors of attitude, beliefs, intentions and behaviours.

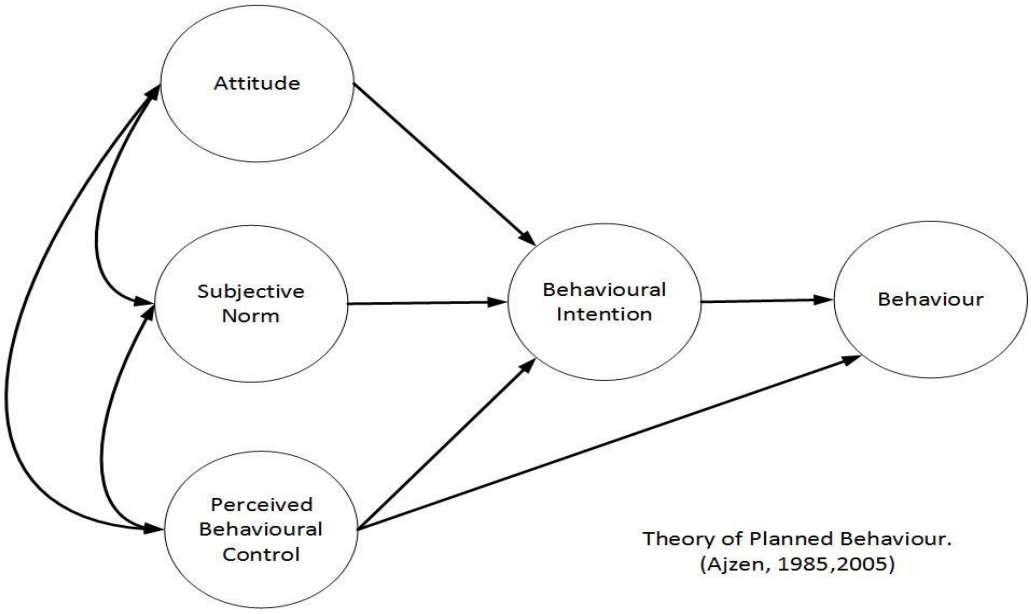
In accepting that trust involves an element of risk or vulnerability the trust relationship affords the benefits of security to the trustor, and to a lesser degree the trustee as well. The presence of trust in relationships leads to the phenomenon that Mayer et al. (1995) described as *'Risk Taking in Relationships (RTR)'.* Trust is instantiated within the context of a risk taking relationship, which incorporates the antecedents; the boundaries to the trust bond; the constraints that act upon it and the internal and external information requirements for outcomes to be achieved. Trust engenders confidence in parties that allows risk taking behaviour to be undertaken with the benefits of a safety net in case of unforeseen exigency.

Trust is a flexible, dynamic and changing relationship continuum (Rousseau et al., 1998; Fukuyama, 1995) and although the core attributes of trusting trustors and trustworthy trustees have been analysed in isolation in the previous section, the emergent system that constitutes the relationship also requires analysis. The relationship represents a confluence of factors across time, electronic and physical space where the conditions for formation are in a constant state of flux. The development, building, maintaining, decline and possible resurfacing of trust relationships reflects this environmental cauldron of factors.

2.14 Risk Taking Relationships Introduction

To understand the transition from decision making to behaviour the widely cited Theory of Planned Behaviour (Ajzen, 1985) has proved significant in framing the motivating factors underlying behaviour by positing that people's behaviour follows reasonably from their attitudes, beliefs (subjective norms), the perception of the amount of control they have, and intentions. This is shown in Figure 2-2.

Figure 2-2 Theory of Planned Behaviour



A critical analysis of the mechanisms of the Theory of Planned Behaviour with respect to the formation of relationships involving trust and risk is presented in this section, where the influencing factors and characteristics of these dispositions are examined to discover their relevance to each other and their contributions to relationship formation where risk taking behaviour leads to outcomes for the participants.

2.15 Attitude

Trustworthiness evaluation is carried out as part of processes that shape the parties' perceptions of each other. Trustors' attitude arises from the evaluation response to the trustworthiness attributes of a trustee and can include cognitive, affective and conative components (Ajzen, 2005). Attitudinal mechanisms to divine the trustworthiness of others is an ability that is developed as a result of evolutionary

processes designed to impose or reinforce normative behaviour patterns that promote and protect relationships in collective action situations (Berg et al., 1995). It arises from both the disposition of the individual and as a result of past experiences (Rotter, 1980).

The result of the assessment of trustworthiness in others is the trusting stance (McKnight and Chervany, 2002) which incorporates the strategy that the trustor will take. A person's attitude toward an object predisposes the overall pattern of responses but need not result in a given action (Ajzen, 2005; Ajzen and Fishbein, 1975), and the factors that influence attitude are critically analysed in terms of the evolutionary imperatives for trust; the evidence of communication and cooperation from game theory experiments; and how trustworthy environments help the fostering of communication and shape the trustors' trusting stance.

2.15.1 Evolutionary Approaches

The historical origins of trust have their roots in the behaviour and responses to survival in early societies. Although survival is, in part, dependent on individuals seeking returns, the need for societal living and collective action to solve problems, either through hierarchical structures or interaction with other co-operating or competing groups meant that individuals who could recognise deceit in others and who could be relied upon was an essential survival skill (Ostrom ,2014).

The duties and obligations of trust in social contexts means that socially oriented parties reason differently about what is permitted, forbidden or required and in

formulating reasons to trust they will check for violations and cheating behaviour before granting trust (Manktelow and Over, 1991). This is in contrast to egotistical reasoners who will rationalise the utility of a relationship primarily based on the economic benefits (Lyons and Mehta, 1997). The evolution of cultural values meant that the adoption of trustworthy values was viewed as a social obligation, and that individuals would also learn the egotistic centred values of material reward. Parties in the modern world incorporate both of these behaviours. Self-interested trust (SIT) is forward-looking. Self-interested trustors will generally be led by the value salience and integrity of trustors to avoid misplaced confidence. Socially-oriented trust (SOT) has its roots in the past (Lyons and Mehta, 1997). Socially-oriented parties will be generally reassured by the relationship history, as this shows that trust has been earned and that the trust was reasonable in review, and values known groups over new parties where no history is present. Self-interested parties are more likely to use that history for personal development of new territories whilst relying on history to forge reputation beyond the group.

The cultural evolutionary process is analogous to a game theoretic situation where the most successful strategies will become more prominent over time, and biological research suggests that the presence of oxytocin in game participants increases the propensity to trust (Zak, 2008). Evolution and biology have developed strategies for parties to interact in social groups in co-operative and competitive situations. To realise these social strategies it is necessary to communicate, and this is explored in the next sub section.

2.15.2 Communication

The study of what has been called pre-play communication on the effectiveness of reaching stable equilibrium states in multi-player games has enabled researchers to investigate the relative merits of strategies that involve self-interested, socially-interested and imposed communication (Lyons and Mehta, 1997).

Trust involves the co-operation between partners who exchange views in a one way or two-way communication, and the relevance to the study of trust is greatest in studies of co-operative games. In co-operative games players seek to form coalitions to maximise the payoff and this is divided between the coalition members in various ways. Coalitions will only form where the individual player cannot get more by playing on his or her own (Rabin, 1993). In terms of trust, coalitions are more likely to form where there is the expectation of a positive outcome.

There are inconsistencies of outcome in cooperative games, and this suggests that there are other factors in play than rational self-interest. Game theory experimentation has shown that *"The success of those who adopt social norms strongly depends on their capacity to identify one another. Thus, contextual variables that enhance the knowledge that players have about each other's past behaviour are theoretically strong candidates to include in future efforts to explain the origin of collective action."* (Ostrom, 1999: 4)

Communication in the pre-play stage of games reduces the time taken to reach equilibrium by promoting coordination (Mailath, 1998). It has been shown that

increases in the levels of co-operation happen when individuals are permitted to communicate face-to-face (Robert et al., 2009), with assessments of trustworthiness based firstly on matching the characteristics of others. Behavioural assessments follow later on in trust formation. They discuss optimal strategies, extract promises and voice disapproval if promises are not met, which discourages both selfish behaviour and the free rider problem where players can reap rewards without contribution (Ledyard, 1995). Similar cooperation strategies have shown that half of participants in public goods games are conditional co-operators and a third are classed as free riders. (Fischbacher et al., 2001).

The assessment of trustworthiness via two-way and face-to-face communication and the discussion of acceptable social norms prior to exchange is a way of using trust as a social control mechanism. Trust acts as a social lubricant and opener up of social capital that encourages contribution, cooperation and reciprocity in relationships (Anderson and Jack, 2002). It also empowers normative punishment and disapproval of transgressions provided that the correct environmental conditions exist for the exchange of views prior to the behavioural instantiation of trust. Environments and environmental factors for the generation of risk taking relationships are examined in the next section.

2.15.3 Environments

Environments that traditionally fostered reference points for trustworthiness were gathering places, familial and tribal groups where communication could happen

away from the urgency of transactional necessity (Bohnet et al., 2010). The spaces where individuals or small groups of people met allowed the sharing of information on values and vulnerabilities to be exchanged. Where information is shared between parties trusting relationships allow the advance of outcomes through that shared information rather than by fiat (Barber, 1983). The trustworthiness of parties can be assessed through the attitudes displayed with face-to-face interaction, and emotional and affective cues contribute to the assessment of trustworthiness (Johnson and Grayson, 2005).

However, translating the tribal meeting spaces to electronically mediated spaces and the sharing of information through multiple channels allows information signals to be synthesized to produce new knowledge (Doan et al., 2001) by combining multiple data sources. This synthetic knowledge and metadata about private meetings means that there are boundary risks for trustors in such information sharing (Sweeney, 2002). If the boundaries of authorised parties to trustworthiness arrangements are widely known, they run an exposure risk whereby other parties may be able to infer that trusting pre-play communication behaviours are in progress. The assertion by Mayer et al (1995:714) that trustors signal a *"willingness to take a risk in the relationship and to be vulnerable"* means that risks are inherent in trusting relationships. If external knowledge of this willingness becomes known it may produce exposure to opportunism, outsiders or a normative backlash from other trusted parties.

2.15.4 Attitude Summary

Attitudes that have developed over many generations of cultural evolution produced a heuristics based process by which individuals weigh up the appropriateness of behaviour in trusting contexts. These heuristics are used as a way to seek the optimal outcomes from exchange, but are accompanied by exposure and normative risk in the event that the privacy of the environment in which trust is formed is exposed. To evaluate trustworthiness the vulnerability of the trustor must be respected in the environment in which they interact with the trustee. A further exploration of the digital equivalent of attitude and trustworthiness evaluation is covered in Section 2.24 .

The way in which attitudes are influenced by shared norms is discussed in the next section, where the influence of history, values and contracts are examined in greater depth.

2.16 Subjective Norms

As covered in the last section, the formation processes involved in trust entail evaluating the trustworthiness credentials of a trustee by a trustor. This decision to trust does not necessarily lead to behavioural action and in such cases agents may make a prior commitment that is not immediately purposive (Origgi, 2004). The behaviour of 'banking' commitment to use later is seen where a party may engage a trustee ahead of the need to be in a trusting situation as *"The fundamental difference between trust and trusting behaviours is between a willingness to assume risk and*

actually assuming risk. Trust is the willingness to assume risk; behavioural trust is the assuming of risk" (Mayer et al., 1995:724).

Belief generation and evaluation for decision trust is moderated by the attitude of the party that is giving trust and the importance of the matter at hand. The decision to trust is neither based on purely rational cognitive or calculative grounds, but accommodates the history, benevolence and salience of values embodied in a partner. When considering decision trust online consumers rely on subjectively assessing the convergence and congruence of values from trustees. The evaluation dimensions encompass history; evaluation of the trustees' values and adherence to normative shared values; and the contracts, compacts, pledges or promises that govern the future of the relationship. These influencing variables on the trust decision are considered in the following sub sections.

2.16.1 Shared History

Actions and interactions between parties leaves traces of history that cannot be unlived, and the persistence of these historical transactions, information, data and metadata is utilised by trustors in the review and evaluation of those trusted actions. Where there is no previous history between parties it is possible, in the online and offline world, to find trustworthiness sources that guide the decision to trust (Schilke and Cook, 2015). Online, there are many recommendation systems available, as the internet has grown from searching and browsing to interacting, creating and sharing content (Zhou et al., 2012). Where strong-tie word-of-mouth recommendation from

family or immediate group was once a scarce commodity there exists a widespread library of weak-tie online resources from acquaintances or strangers with which to evaluate the trustworthiness of others (Duhan et al., 1997).

Although trust cannot be willed, it is possible for organisations to create structures to make trusting successful to enhance their trustworthiness (Hardin, 1996) and in so doing seek to be contained within the class of valued, trusted providers known by the trustor, and whose inclusion in that class is determined by the trustors attitudinal and relational propensity to trust.

Although it is possible to consider trust as constituting repeated positive interactions and trustworthiness represented as an accumulation of perceptual experiences that leads customers to trust the service provider (Caldwell and Clapham, 2003) there are other sources of information that potential trustors consult and this places influencers and modifiers into the decision trust process. The perceptual experience is dependent upon prior communication or contact with the service provider with which to evaluate that experience. Although transactional services may have been carried out in an environment of trust, it may only be discernible in hindsight (Anderson and Schalk, 1998).

The cognitive processes involved in evaluation can take time to assess, and trust decisions are sometimes based on limited time, knowledge and computational capacities (Ahituv et al., 1998). The study of bounded rationality (Simon, 1955) examines how decisions are made where sub-optimal information is available to the party. Decisions under such conditions can be made by taking into account the

psychological plausibility of an action based on the cognitive, emotional, social and behavioural repertoire of the agent and applying domain heuristics relevant to the situation. This often requires utilising rules from similar domains to select an option. Ecological rationality relates the domain specificity to the heuristic to decide if it is the optimal strategy that matches the structure of the environment. To avoid cognitive inertia the agent decides stopping rules for cognitive thinking before inferring an action that may be appropriate for the situation at hand (Gigerenzer and Selten, 2002).

Transaction history is important to both parties in a relationship not only as a measure of the ability of the trustee to deliver outcomes, but when used for refund, dispute resolution or reimbursement purposes it can also be used as the yardstick to measure the integrity and benevolence of the parties. In many cases where uncertainty is present historic behavioural trust is used as an antecedent of future decision trust to save the cognitive stress of forming new relationships and can aid the trustee by depending on reliance focused trusting that allows parties to make fast, frugal and computationally cheap decisions (Gigerenzer et al., 2002). The repeated interactions of operational trust demonstrated by economic theorists may result in the deeper, socially rooted trust described by sociologists (Axelrod, 1986) by interpreting past interactions as involving measures of benevolence towards the trustor. Thus, the immediacy of transactional trust may lead to a more longitudinal form of relational strategic trust that affords a wider margin for error and incorporates

greater leeway in the granting of discretion, tact and forgiveness within the relationship.

The dimensions of trustworthiness are not always given equal prominence where trust has been violated. If the violation concerned lack of ability then perceptions of competence were lower than perceptions of integrity. When violation concerned integrity then perceptions of integrity were lower than those of competence (Kim et al., 2006). Although successful outcome is an important rational measure trustors also view the relationship interactions dependent upon their affective mental states. Research has shown that these mental states can colour interactions in which a trustor was a protagonist as more positive than negative depending on subsequent life scenes (Wildschut et al., 2006). Betrayal aversion and fear states can similarly produce negative interpretations of what may be the same events (Koehler and Gershoff, 2003). The inaccurateness of perceptions can result in the reinterpretation of seemingly unambiguous events and aid consumers to enhance social bonds and self-regard at the expense of rationality. The presence of two-way communication and the revision of experience through the prism of emotions calls into question the viewpoint of trust as a 'historical residue' (Fisman and Khanna, 1998), and the irrationality of emotions provides dynamic viewpoints of historical events. This suggests a line of enquiry that makes some beliefs compelling and others not (Greenspan, 2000; De Souza, 1979), the cognitive sets enabling or disabling decision beliefs beyond the confines of rational reasoning.

The historical traces of trust can be used to evaluate the dimensions of ability, integrity and benevolence of trustworthiness in past episodes of trusting behaviour, and the rational facts of past transactions may be coloured with the aversive or enabling interpretation of these attributes by trustors. In addition to history, shared values also play a role in the assumption of risk, and these are covered in the next sub section.

2.16.2 Shared Values

Some definitions of trust emphasise the observation that it is made under conditions of risk where incomplete information is available about either or both the task and the trusted party that is to be entrusted (Lewicki and Bunker, 1996; Tomkins, 2001). Thus, trustors will endeavour to extrapolate any knowledge of past interaction with respect to attitude and norms to arrive at a subjectively reasoned trusting intention.

A trusting relationship also involves elements of commitment. Commitment involves one or more of three distinct processes. These are compliance, identification and internalization. Internalisation of values reflects the acceptance of influence by another individual because of a perceived similarity in values (Coughlan, 2005; Kelman, 1961). In this regard, a consideration of the values of an organisation is one way of predicting how a trustee will behave in future unspecified situations because of the relative influences of economic, ethical, environmental and political priorities (Barnett and Karson, 1987). The role of values is as *"determinants of virtually all kinds*

of behaviour that could be called social behaviour or social action, attitudes and ideology, evaluations, moral judgments and justifications of self and others, comparisons of self with others, presentations of self to others, and attempts to influence others." (Rokeach, 1973: 5) Values transcend specific contexts and have to do with modes of conduct and end states of existence. Particular modes of conduct or end state are personally and socially preferable to the alternatives. Modes of conduct are guided by instrumental values such as courage, responsibility and honesty, and end states are guided by terminal values such as peace, equality and harmony (Rokeach, 1968).

Siegriest et al., (2000) proposed that social trust is evoked by the saliency of values (Salient Value Similarity) to the matter at hand. The perceived agreement between parties where different kinds of values are salient depends on whether the issue is of high or low concern or importance. A situation of high concern leads to a high motivation for trustors to trust and vice versa. In dealing with the uncertainty of trusting parties who may prove to be unreliable the contribution of salient values similarity lies in providing a strategy to trust for trustors who sense that trustees will follow what they consider to be appropriate guidelines and general principles for setting goals and procedures. Research examining trust in buyer-seller relationships found that it is fostered because buyers feels better able to assess the salesperson's intentions and that buyers attribute benevolent intentions to "similar" salespeople they believe share their values and this makes it easier to predict behaviour in future situations (Doney and Cannon, 1997; Sirdeshmukh et al., 2002).

The role of communication in sharing information in a timely and meaningful way, informally and formally, has been shown to foster trust by helping to resolve disputes and to facilitate the alignment of expectations and perceptions (Morgan and Hunt, 1994; Anderson and Narus, 1990). This dependence on information requires having a reliable information source to provide epistemic vigilance, and a reliable informant must meet two conditions; they must be competent, and they must be benevolent (Sperber et al., 2010). The same informant may be competent on one topic but not on others, and benevolent towards one audience in certain circumstances, but not to another audience or in other circumstances. Taking into account the contextual cues of topic, audience and circumstances makes decision trust based on information a costly cognitive exercise. Trustors may fall back on the less costly alternative of general impressions of competence, benevolence and overall trustworthiness dictated by values. Values help to differentiate trust as exogenous dependence in a 'generalised other' into endogenous social trust and thus subject to change (Mutz, 2005).

Having considered the role of shared values in the commitment to a risk taking relationship, the next sub section looks at how these are realised through the role of shared contracts in the relationship.

2.16.3 Shared Contracts

To counteract the uncertainty of interpersonal actions formal structures can be used that place constraints on the boundaries of the interaction context. These formal

structures can take the form of contracts, hierarchies, networks and controls that aim to reduce the risk of interdependence (Sheppard and Sherman, 1998). In place of contracts informal trust structures include the giving of promissory contracts containing elements of promises, payments and acceptance. Promises communicate commitment to future action, payments help to ensure the keeping of those promises and voluntary acceptance seals the commitment to act. In sum, all contracts are expectations, but not all expectations are contracts (Rousseau and Parks, 1993).

As shown in the prior sections, generating trust requires gauging the trustworthiness of the resource owner and an appreciation of the situation (Williamson, 1993). In situations of high risk the adoption of 'blind trust' is not a suitable option for the resource owner, so contracts and hierarchy seek to impose compliance on the trustor. Contracts form an institutional solution to facilitate exchange by helping to reduce uncertainty, eliminate risk, and enhance control (Malhotra and Murnighan, 2002). The enforcement of contract enhances the probability of positive outcomes by imposing obligations on the parties to a trusting relationship and in so doing delineate the boundaries more closely. Although a contract is sometimes able to take the place of trust it is not able to effectively cover all eventualities and a mixture of formal contract and informal trust relationships may be necessary. The presence of contracts imposes restrictions on behaviour that can help to reassure low trusting parties that controls are in place, but the effect of controls may become weaker in high trust situations. The loss of control in high trust

environments may lead to an increase in coordination concerns as high trust environments make more use of delegation (Mellewigt et al., 2007).

Contracts have different effects on building mutual confidence against exploitation, moral hazard or holdup, or any other vulnerabilities that may exist in an exchange (Barney and Hansen, 1994). Contracts can enforce a weak-form trust, where few opportunities to break trust exist, whilst strengthening a semi-strong form trust through governance that increases the economic cost of opportunistic behaviour. Where a strong-form trust exists, it is regardless of the vulnerabilities of the exchange method due to internalised values, principles or standards. Trustworthiness in strong form trust relationships is because it is rooted in internal attitudes and avoiding costs is not the primary reason for trust.

Regulation and enforcement of breaches of trust builds confidence in successful outcomes by enforcing the structural assurance and normality of the exchange context (McKnight, 2000). Regulations and controls impose institutional governance through the use of policies and provide the prescriptive responses and guarantees of service that can be taken in the event of breach of contract (Clague et al., 1996). Regulation allows the boundaries of the risk taking context to be defined more precisely, and management allows normative decision making to take precedence over automated decision making that may not necessarily reflect the wishes of the customer. Traditionally specialized control mechanisms include price and authority. Price mechanisms are sometimes built into hierarchies of authority, and authority mechanisms sometimes bind independent exchange partners in a market by helping

to reduce transaction costs (Bradach and Eccles, 1989; Eccles and White, 1988). The imposition of hierarchy may involve the installation of an authority relation between the contracting parties that may be less costly than an arms-length market transaction. The networked structure of electronic organisational exchanges has seen an expansion of websites that act in the role of authority to connect parties directly through the mechanism of acting as information intermediaries (Xiang and Gretzel, 2010).

The traditional custom of signing contracts with the shaking of hands lends the weight of normative behaviour codes to the contract situation to put trust in practice (Shapiro et al., 1992). In particular, norms, standards and obligations harmonise conflict situations through shared or explicit understanding and the preservation of the trust relation for broader social and economic well-being (Bradach and Eccles, 1989). The anonymity of contract signing online and the difficulty of determining the terms and conditions attached to such contracts in electronic spaces may lead to a withholding of decision trust (Lewis, 2011).

The promises of contract reassure and provide security to trustors in their evaluation of trustees, where the contracts are voluntarily accepted and where the hierarchies and controls on the trustee organisation can help to ensure that vulnerabilities are not exploited. The benevolent behaviour of trustors is shown by adherence to business ethics, showing goodwill and demonstrating good citizenship (Moorman et al., 1998). The imposition of contracts and governance mechanisms help

to define the context of the relationship and the expectations of both parties to the relationship.

Contracts allow trustors to act without having to worry about the support to achieve their goals being withdrawn, and controls are exercised to balance an optimal level of rational prediction. The rational constraints of contract and control combined with belief in moral character helps to assure trustors of the integrity and benevolence of the other party. How these beliefs are generated are explored in the next section.

2.16.4 Subjective Norms Summary

This section analysed the granting the willingness to trust as the outcome of socio-cognitive dynamic processes. Prior experience of exchange between the trusting partners provides exemplars of trust behaviour with which to influence future decisions. Value congruence attests to the shared goals and preferred processes that demonstrate integrity by adhering to social norms. Contracts, implicit or explicit, contribute to the evaluation of trustworthiness by demonstrating good faith and fiduciary responsibility.

However, rational assessment only takes the analysis so far. Trust allows trustors to act as if uncertainty is reduced without reducing the actual uncertainty involved in taking action (Tomkins, 2001). Providing individuals with assurance of ability, integrity and benevolence from partners without the need to monitor the relationship only requires information on those particulars of the relationship that were not given on trust, and there is an inverse relationship between the willingness to trust and the

need for information (Wicks, Berman and Jones 1999). In situations of uncertainty reduction, subjective norms are used as an alternative to information in addressing vulnerability.

Trust is generated from a combination of the specific beliefs of the trustor in the trustworthiness of others and the decision to trust reflects this belief. To generate this belief trustors will use search capabilities that communicate the ability to provide the expected outcome, and intentions are directed by the perceived integrity of a potential partner (Gefen, 2008).

The presence of trust within a dynamic relationship argues against the adoption of a static equilibrium based approach to trust, focussing instead on the *"developing, building, declining and resurfacing"* (Rousseau et al., 1998: 395) of trust based on historical reviews of the subject. Trusting relationships are defined by focused intent directed towards goals or a desired end state, and these are made relative to the constraints on the situation. Communication of social norms through information systems decision support is covered in Section 2.26 and the behavioural control mechanisms that give trustors the motivation to translate their beliefs about social norms and attitudes into the intention to trust is described in the next section.

2.17 Behavioural Control

The balance between attitude and social norms in taking the decision to trust is an individual choice mechanism, and this relies on setting the boundaries of the relationship. This results in the controlled behaviour variable, described as a belief

that an individual has in whether they have sufficient skills and information with which to carry out a task. It involves acknowledging the boundaries of capabilities and involves the psychological motivation for trusting action and setting controls on what the interaction involves.

2.17.1 Behavioural Motivation

The basis for the decision to trust is relational, and the thinking processes that potential trustors execute is drawn from the Heideggerian concepts of 'Dasein' or care, in being a practically engaged being in the world (McConnell-Henry et al., 2009). The act of thinking is reflection based on our experiences of making our own way in the world and in seeking care from trustees that allows for widened 'possibilities for being'. The willingness to be vulnerable stems from the search for closing such possibilities for time (Richardson, 2013).

Based on the need for care in a context a trustor has to know that they can display a willingness to trust another party without advantage being taken. The commitment to trust is generally perceived to be enduring, and as such represents a positive valuation of a relationship that will not change often. Trustors are unlikely to make such commitment to something that they do not value (Moorman, Zaltman and Deshpande, 1992), and will base relationship decisions based on their perception of that value (Sirdeshmukh et al., 2002). As the trust bond is perceived to be a longstanding commitment it is necessary to control the boundaries of the relationship. It could be said that as trust controls, it requires trust controls.

2.17.2 Perceived Control

The combination and weightings of attitude and subjective norms is appraised by the individual, with attitude being concerned with the assessment of behavioural consequences, and subjective and group norms taking into account what others may think about that behaviour (Pavlou and Fygenson, 2006; Madden, Ellen, and Ajzen, 1992). The weighting, or power, given to the influence of attitude and norm are used to calculate the ease of following a particular behaviour using perceived behavioural control (PBC) evaluations and determining the subjective ease of performing the possible behaviours.

Attitude and social norms are surfaced through the trusting stance taken dependent upon the situation in hand. The stance adopted by a trustor is, in part, down to their assessment of the perceived trustworthiness of the exchange partner, and partly due to the influence of cultural evolutionary strategies, with trust influencing behaviour by acting as both an attitudinal and control belief. Perceived control also takes into account motivation. If people believe there is little control over trusting because the resources to do so do not exist, then their intention may be low, even when their trusting stance is high. Therefore, the perceived behavioural control over whether to trust is strongly influenced by the confidence individuals have in being able to perform the task (Bandura et al., 1980). This is related to both the system and party elements of trust delegation. The recursive nature of trust is felt as an antecedent of both attitude, due to confident expectations, and controllability, due to uncertainty reduction (Pavlou and Fygenson, 2006).

2.17.3 Behavioural Control Summary

Risk and trust are two tools with which to make decisions in uncertain environments and are part of the socio-cognitive decision making process. These reasoning tools are given relevance and importance within the context that an agent is considering action. The two concepts are related, and "*Risk influences Trust, but context influences actions*"(Gambetta, 1988). Risk approaches to decision taking require agents to take into account the expected value or expected utility of decisions based on an analysis of the probability of the successful outcome to a transaction in making the decision to proceed. Whereas risk evaluation based methods are rooted in probabilities of transaction failure, trust based decisions are based on the possibilities of dependence and uncertainty of reliance on another party (Jøsang and Presti, 2004). Trust decisions are based on possibility measures and risk is based on probability measures of uncertainty determination. The perception of risk moderates the relationship between trust and risk taking (Schoorman et al., 2007) and the perceived probability of success or failure of a transaction makes trust relevant in situations where a party must enter into risks but has incomplete control over the outcome. Therefore, as trust increases, consumers are likely to perceive less risk than if trust were absent (Kim et al., 2008).

Whereas intentions reflect a willingness to try and enact a certain behaviour, controls exercise constraints on that action. Controls on whether intention is carried through in behaviour depend on internal factors and external factors. Externally, the presence of means, opportunity, and motive have been forwarded as the drivers for

behavioural choices (Pendse, 2012), and trustee ability is an external factor that trust seeks to resolve through partnerships (Mayer et al., 1995). Factors such as forgetting (Pomazal and Jaccard, 1976), strategic ignorance (McGoey, 2012), and the emotional aversive responses to betrayal and mistrust (Koehler and Gershoff, 2003) have been posited as internal controls on behaviour. The cognitive effects of perceived behavioural control (Ajzen, 1985) define a space where the presence or absence of resources and opportunities taking account of past experience and second hand information with which to assess the perceived difficulty of action through behavioural control.

2.18 Intention

The development of trusting belief is an antecedent to the willingness to depend on another party and trustors show beliefs through their trusting intentions. Although there is a confident expectation that delegating tasks will produce a positive outcome trusting parties may also experience negative consequences due to dependence, lack of control or the negative effects of the actions of the trustees or their agents.

An intention to trust reflects reliance on another party to secure outcomes and this involves delegating actions that may involve increased vulnerability to the trusting partner and the uncertainty of outcome that arises from actions. As *"the emotional basis of trust provides continuity with rationality"* Barbalet (2009:382), trustors believe the positive expectations will be met and voluntarily place resources at the disposal of another or transfer control of resources to another (Coleman, 1988). The control

that is passed to trustees is not unconditional, it is bounded with the intention of the trustor. Except in the case of 'blind trust', the trustee is tasked with achieving outcomes for the trustor.

Therefore, the aims, objectives and plans of the trustor delineate the boundary of the trusted engagement and the characteristics of intentions, goals and how these are achieved through delegation of authority are discussed in the following sub sections.

2.18.1 Reasoned Intentions

The intention of the trusting relation is to communicate the objectives that the trustor requires and that the trustee should perform. The relevant mental state of belief of the trustor is given external significance through intentionality. Types of subjective mental states held by individuals can include belief, desire or fear, and these are captured as the intentionality to do something, that is, the internal mental states are given external significance in the intention to act towards goals in a mind-to-world fit (Devlin, 1995; Searle, 1983). Success is measured in terms of the world-to-mind fit of the intentionality of thoughts. That is, if the goals of belief, desire or fear of the intention is met then the aim of trusting has been achieved. Intention is satisfied if, and only if, the belief or desire is fulfilled through intentional action. Intention is carried through to realise the beliefs or desires through actions. There is no action without intention, but there exists an asymmetry within which there are intentions

that are not always accompanied by actions, which explains the phenomenon observed by Origgi (2004) of banking commitments to trust in advance of action.

2.18.2 Goals

The establishment of common goals to the trust relation depends on the communication between the parties. Goal setting is used to realise the aims of trusting behaviour, through the planned realisation of aims, objectives and outcomes by the achievement of proximal milestones. Goal setting is important in directing behaviours that are concordant with the planned behaviour that is expected to produce outcomes. Intentions are composed of behavioural dispositions until, at the appropriate time and opportunity, these intentions are translated in to action (Ajzen, 2005) and intentions delegate the control of goal directed responses to anticipated situational cues (Gollwitzer, 1999).

Research evaluating the TPB and the correlation between intention and behaviour suggests that there is a strong association between intention and behaviour (Ajzen and Fishbein, 1980). Studies relating to the intention-behaviour relationship where behaviour is non-volitional tend to suggest that this correlation is lower (Sniehotta, 2009), and where the transition from intention behaviour is contingent on the actions of delegated agents with other commitments or conflicting goals

(Castelfranchi and Falcone, 1998). In a risk relationship the trustee's actions need to reflect shared goals that the trustee can encapsulate as their own. The goals of the relationship, where time pressure is not critical, is deliberated on prior to taking action. This allows the parties to consider the consequences, implications and expectations of the proposed behaviour prior to the commitment to proceed.

As behaviour is goal directed (Einhorn and Hogarth, 1981) the formulation of plans and objectives and their associated goals must match the expected outcome that the trustor feels will reduce the vulnerability inherent in trusting action. In online environments trust is likely to be rooted in impersonal weak or thin trust ties that are perceived as being riskier than reliance on thick interpersonal ties (Khodyakov, 2007; Granovetter, 1973). The similarity and interests of shared goals through trust can assist in strengthening the trust and identification bond between the parties when successful. Intentions and goal setting may be bypassed if the trustor is well practised in taking decisions in the domain in question. To save cognitive effort, actors may make intuitive decisions that lead directly to action without the need for reflection or prolonged information gathering (Kahnemann, 2003).

The intention of trusting involves not only self-reliance but goal directed reliance on another party and it is therefore essential to examine the role and nature of action delegation and the ways in which it enhances or undermines the mechanics of trust.

2.18.3 Delegation

To carry out tasks on behalf of the trustor a trustee may act in a role of delegated authority, acting as a proxy for the trustor. Contracting through delegation to others involves instigating action, not just a decision, and in delegating a task to another agent the trustee is creating a new social relation to achieve a goal. Research in organisational settings showed that trust contributed to managers' taking greater risks in their relationships with their employees. This was achieved through increased delegation of authority to trustworthy employees (Schoorman et al., 2016; Mayer et al., 1995). Trust is neither necessary nor sufficient for delegation, and delegation without trust may happen in cases where the delegated agent is not free to choose, where there is information asymmetry or where there is no choice (Castelfranchi and Falcone, 2005).

Delegation can be classed as being weak or passive, where the delegated agent is not aware of being used, or strong delegation where the agent carrying out the task is dependent upon adopting the beliefs or goals of the principal. Where strong delegation takes place, this is made in part on the ability of the delegated agent and consumers can employ a strategy where decisions are delegated to the agent, with the agent acting as a surrogate customer (Aggarwal and Mazumdar, 2008). Where decision delegation takes place the agent assists in attribute identification to decide on product features, choice set reduction, and final choice decisions where the selection of products is fully automated. The adoption of online environments for commerce has meant that this service is increasingly being offered by vendors.

Delegation introduces an agency problem. According to agency theory, a principal-agent relationship exists when one party, the principal, contracts with another party, the agent, to perform a task involving delegation of decision making in exchange for compensation (Eisenhardt, 1989). Delegating agency to another is used as a risk sharing strategy but can become problematic. The first is that the desires or goals of the principal and agent conflict, and it is difficult or expensive for the principal to verify what the agent is actually doing. The second is the problem of risk sharing that arises when the principal and agent have different attitudes toward risk. The problem here is that the principal and the agent may prefer different actions because of the different risk preferences (Eisenhardt, 1989; Johnson and Grayson, 2005). Agency depends on the transitive nature of trust from the principal to the agent and this may cause security and other protection problems where the agent is not aligned with, or respects the principals' goals (Waterman and Meier, 1998).

2.18.4 Intention Summary

Intentions are used to direct and direct behavioural actions towards objectives. Trusting relationships utilise cooperative behaviours to achieve the ends of their endeavours, but this comes at the cost of the loss of independent action and volition.

Although reasoned action can be shown to correlate to behavioural intention, there is often an intention-behaviour gap between stated intentions and actual behaviour. This can be driven by external or internal factors that prevent action being taken towards goals, and the goals of the delegated trustee may not be aligned with

the intentions, beliefs and attitudes of the trustor. The premise that trust involves the ceding of control without the necessity of monitoring other parties involved in action can lead to behavioural risks being incurred, especially where the risk threshold between the trustor and trustee diverge. To help minimise the risk of behavioural action the intention to act is communicated by passing signals about values or signing contracts between parties that describe the boundaries, goals and intentions of action.

In managing the complexity and risk associated with actions the next section examines the realisation the benefits of actions by considering the implications of behavioural action and how this is enabled through the formation of trusting relationships.

2.19 Behaviour

The transition from a decision to trust to the behavioural manifestation of that trust involves the formation of an active trust relation, and by enacting relational exchanges it yields benefits to both parties of the relationship. It has been argued that the cognitive process of decision trust does not involve risk as it encapsulates only the willingness to be vulnerable (Mayer et al., 1995). Therefore, risk is assessed not on the possibilities of the relationship, but on the behavioural manifestations of the willingness to be vulnerable. Actions involve engaging with risk and the trusting behaviour or 'risk taking in a relationship (RTR)' (Mayer et al., 1995) is the mechanism

by which the decision to trust is manifested in situations and is where one party behaviourally depends on the other party (McKnight, 2001).

Behaviours consist of four different elements. These are:

- The Actions taken.
- The target at which the action is directed.
- The context in which the action is performed.
- The time at which it is performed. (Ajzen and Fishbein, 1975).

An examination of the influence and role of how intentions are manifested in behaviour require reference to the actions, targets, contexts and timing that are influencers on the desired outcomes, and these are described in the following sub sections.

2.19.1 Actions

Actions are carried out to instantiate the aims of intention or belief (Searle, 1980). Directed action by utilising a trustee or a delegated agent enacts changes in the external environment for the benefit of the trustor, whose goals should be encapsulated by the trustee in the work they carry out. Researchers have noted an 'intention-behaviour gap' in the context of customer's ethical behaviour (Carrigan and Attalla, 2001). Purchases are made based either on beliefs or purchase intentions been noted, (Pavlou and Fygenson, 2006), and this suggests that either belief or reasoned intention can be the driver of behaviour.

Implementing changes involves accepting the risks associated with the uncertainty of the outcomes such action will produce. This uncertainty is communicated to the actors through the entropy of information received from the target of the action. This information constitutes one of the outcomes of behavioural action. The information perspective of action also entails trusting the agent that gave the information regarding the action taken (Tan and Theon, 2000). Action can be viewed, not only as a dependent variable of the cognitive process but is *"an independent, creative variable, involved in constructing, shaping, and modifying all other social objects, including social wholes of all sorts: groups, communities, societies."* (Sztompka, 1999:3).

Outcomes arise out of action taken in contexts and the record of results provides an understanding of the path dependent processes of relationship trust that build upon each other and provide opportunities for reflexive review. Therefore, an examination of the influence of context on action and outcomes is required, and is covered in the following sub section.

2.19.2 Contexts

The relations between parties engaged in trusting is characterised by bounded contexts in which cooperation and communication takes place and instantiating trust in the context facilitates actions. *"There is both situational specificity and cross-situational generality determining behaviour"* (Rotter, 1980). The level of trust in any situation also depends on the subjective influences of previous experiences and trust

propensity (Tan and Theon, 2000). The cognitive approach has been concerned primarily with how tasks are represented but not why they are represented. Thus, minor contextual changes can lead to the violation of the most intuitively appealing normative principles (Einhorn and Hogarth, 1981) by changing the frame of reference for why tasks are done.

The flow of information between parties is dependent upon the context and meaning of the information passed between them and the basic types of information provided include temporal locations; spatial locations; individuals; relations; contexts and information sets (Devlin, 1995). This represents the information that needs to flow within the situation to accurately model the domain relationship. Context cuts down the information requirements of trust, allowing the parties to agree which information flows and protections are important to their specific service. Since, by definition, trust relationships are less likely to require monitoring the information needs of these contexts is lower and is only restricted to the areas which are not taken on trust (McAllister, 1995). Situations hold many viewpoints and are hierarchical in nature, with each situation containing multiple contexts. By placing situations above context, situations act as a context aggregator (Dey, 2001) and complexity reducer. Situations act as the targets for directed action, and the consequences of action in situations may require contingent actions to be taken (Wright et al., 1996).

Trust is dependent upon the knowledge each party has of a situation, and information asymmetry plays a strong role in the relationship. The asymmetry of information and knowledge is inherent in trusting relationships as trustors face

uncertain outcomes. Information and data are the resources that trustees employ on behalf of the trustor to secure outcomes (Eaton and Bawden, 1991). The use of electronic spaces facilitate the search for information and its' use as an information leveller means that ready access to information may preclude the need for trust. Information is 'the difference that makes a difference' (Bateson, 1970) and the importance of information in building knowledge is in recognising the risk attenuating value of certain information patterns over others. Understanding the domain of action allows parties to become more reliable in their interactions, as the trust relationship moves from an evaluative stage to an accommodative stage (Lewicki and Bunker, 1996). This knowledge is gained by both parties, but the party who has more power in the relationship will likely perceive, by virtue of that power, less risk and, thus, will engage in more risk-taking actions (Schoorman et al., 2007).

Risk taking in contexts requires an idea of time as a sequence and it is an important factor in the development and expression of the belief, intention and behaviour, and is analysed in the following sub section.

2.19.3 Time

In the assessment of trustworthiness contained in this thesis, belief in the other party framed in the construct of '*time as an arrow*', whereby historical factors attest to ability, the present attests to integrity, values and reputation and the future speaks of promises of benevolence. This view of time is reflected in the trust research

literature (Vanneste et al., 2014; Kim et al., 2009; Schoorman et al., 2007; Mayer et al., 1995).

An alternative conceptualisation of time that helps to frame the trust formation process that takes into account the computerisation of interconnected networks of actors can be found in sociological theories of network society (Castells, 1998). Technology has always shaped the social reality of space and time, and the introduction of technologies are key elements of the emergence of organizational forms and managerial approaches. These are required to accommodate and manage the new compression of space and time, a compression that computing has accelerated. Parties are brought together in time without the contiguity of being in the same physical space. This 'Space of Flows' (Castells, 2005) selectively connects places according to their positions as nodes in the network and this changes both their functional logic and social dynamics. People become part of a context where interaction is based on the logic of time sharing in distant places connected to the nodes of a network.

It is, therefore, necessary to look at the interaction between the different temporalities of change cycles. Historically, the introduction and adoption of clocks to track the passing of time led to the synchronisation and sequencing of the activities of people and goods, and management behaviour was optimised to plan and track this. The introduction of network technology that has shrunk time differences between spaces has a knock on effect on the cyclical rhythms of the constructs that lead to trust. The instantaneity of transactions has knock on effects to the planning cycles of

intention, the bureaucratic time cycles of institutions and ultimately the generational cycles of social attitudes. As trust is based on the stability and reliability of social structures the effects of these enduring qualities positively influence the observed trust levels. In electronic environments actions and outcomes are immediate and have relational and sequencing effects beyond the immediate space of the consumer. The differing temporal considerations of organisational alliances can be subject to opportunism and trust breaking (Das, 2006). Organisations have to adapt to opportunity in real time markets, but this may conflict with perceptions of the fair treatment of customers or the violation of accepted social norms (Noe and Rebello, 1996). The assessment and perception of these outcomes is covered in the following sub section.

2.19.4 Outcomes

Outcomes and consequences arise from acting in a context where action is directed at a target towards a goal, with the aim of producing a change in that situation. The results of such actions produce outcomes from the behaviours that can be negative or positive. Where trust is present, the production of outcomes is dependent on the trustworthiness of the trustee (Hardin, 1996) and their actions and motivation to act on behalf of the trustor should reflect the goals of the trustor and give security to reduce vulnerability as a by-product of the trustee assuming risk for the other party.

Some actions are indelible and Arendt (2013) argues that forgiveness is essential to temper the irreversibility of action. Successful action relies on the ability of the trustee in taking the correct actions and shows integrity if the actions are not opportunistic. Taking action allows parties to accrue records through which to assess the health of the trust relationship with subsequent actions widening the relationship scope beyond a single transaction. In taking action the parties are able to demonstrate their trusting responsibilities by demonstrating outcomes from the relationship. Trust moderates the effects of action by allowing communication to happen that interprets the outputs of those actions. Therefore, re-interpretation and selected forgiveness of actions undertaken by another party are a characteristic of trust over reliance in relationships, and this communication channel is what differentiates the outputs of the system from the outcomes.

The manifestation of behaviour bestows the benefits of trust at the cost of increased co-ordination and agency risk, and the acceptance by the trustor of a dependence on the trustee. Co-operation makes tasks more productive and efficient but at the price of vulnerability and threat (Tooze, 2018). In enduring trust relationships the benefits include reducing the transaction costs necessary in exchange, and by leveraging social capital to effect change (Lin, 1999; Fukuyama, 1995). In addition to the benefits to trustors, the relationship benefits trustees by producing longer-term commitments and potentially a continual stream of interaction between buyer and seller (Crosby et al., 1990). Trustee organisations are also able to

benefit from the amortization of costs over multiple exchanges (Chiles and McMackin, 1996).

2.19.5 Behaviour Summary

Behaviours and actions are the exogenous displays of trust made manifest to effect changes in the environment that reflect the beliefs and intentions of the trustor. Customer behaviour is precipitated by the need to take action to reduce vulnerabilities and is contingent upon the perception that a positive outcome will arise from these behaviours. Trust is highly contextual, and the trusting relationship context defines the type of trusting relationship that controls and modifies the externally viewable outcomes.

Actions may be transactional for simpler interactions, but build an epistemology of trusting action. A historical view of transactions builds heuristics with which to face the risk, unpredictability and uncertainty that is present when actions are carried out. Actions have consequences that are not always known until reflected upon, and these feed through the network of trust to affect systems which work on extended temporal cycles. The outcomes of trusting behaviour are the signatures of trust being present and are indicators of the health or otherwise of the relationship.

2.20 Environmental Factors

The electronic environment of interaction is a parallel of the real world of relationship formation where trusting partners need to negotiate the hurdles

presented by environmental confounding variables. Electronic environments present challenges for trusting parties, not least in the adoption of new technology, websites, devices and communication channels (Venkatesh and Davis, 2000; Davis et al., 1989). This multiplicity of environmental changes amplify the need to implement structural and organisational change between partners that can lead to problems of coordination (Power and Singh, 2007).

When comparing an online relationship space and a physical trusting relationship space there are several important points of difference to be made that affect the interactions between parties and that have an impact on the trust forming processes that take place within such spaces. These differences necessitate an analysis of the dimensions and processes that have increased importance in the online environment. Variations are due, in part, to the loss of information that occurs when parties interact without face-to-face discussion, and others are introduced due to the open, multi-agent, distributed and dynamic nature of the supporting environment.

Forging trusting relationships online relies on the provision of several important environmental prerequisites that underpin the safety of the decision making space. For customer to business relationship formation a space must offer guarantees about the Security, Identity, and Privacy of potential relationship participants (Milne, Rohm and Bahl 2004; Miyazaki and Fernandez, 2001; Miyazaki and Fernandez, 2001). It must also distinguish between channel risk, known as internet risk or web risk, and store risk, also referred to as vendor risk (Gefen, 2003). The perceived risk and ease of use of systems that enable electronic marketplaces is also an issue with consumers and

the use of the technology acceptance model (TAM) reflects these adoption concerns (Venkatesh and Davis, 2000).

The widespread use of electronically mediated commerce has lead researchers to investigate the role that the medium plays in motivating users to use the internet. Research has shown that this usage comes with concerns related to privacy related to transaction and individual information (Korgaonakar and Wolin, 1999) and privacy concerns influence customer purchase intent with strong negative effects, both directly and indirectly through trust (Eastlick et al., 2006). Fostering consumer trust also directly affects the effective purchasing behaviour, preference, cost and frequency of visits, raising the level of profitability and decreasing the cost of customer churn (Chen and Hitt, 2002). In addition, trust in the internet is strongly influenced by the security perceived by consumers regarding the handling of their private data (Flavián and Guinalíu, 2006). The possibility of cyberattack imposes a security risk, awareness, protection and communication overhead to the parties and the relationship (Nurse et al., 2011). This need for trustworthy, electronically mediated communication in online environments affects the pre-play communication seen to increase cooperation, and attempts at cooperation, according to the game theory perspective (Cooper et al., 1992).

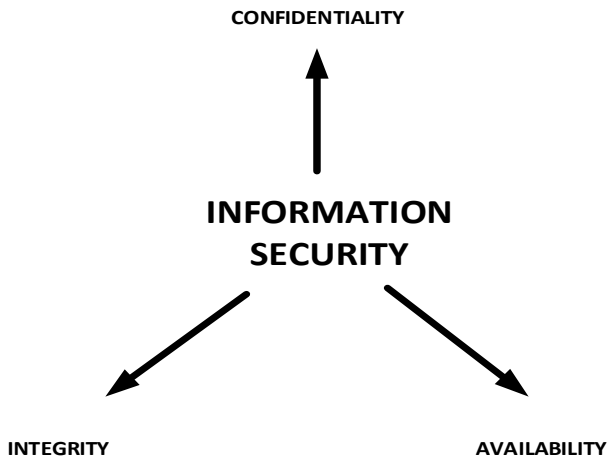
This section compares trusting environments online with those of the real world and highlights the differences between the two. The three relationship environment controls are inter-related but separable parts of the landscape that enable trust

through the protections they give to the trust formation process. They are explored separately and the interplay of these factors is analysed in the section summary.

2.20.1 Security

Information security offers assurances of the confidentiality, integrity, availability and non-repudiation of information messages. These security principles underpin the processes and mechanisms that protects the information that fosters trust at the interpersonal, organisational and societal levels. Information security is a set of procedures, mechanisms, and computer programs for authenticating the source of information and guaranteeing the process (Tsiakis and Stephanides, 2005).

Figure 2-3 The C-I-A Triangle



Securitization of channels is assured by the implementation of encryption, secure protocols and public key infrastructures that are embedded into the sharing of information between the parties (Hoffman, Novak, and Peralta, 1999) and as such the

role of secure communications is essential to the communication of trustor vulnerabilities where sensitive information is being exchanged.

Integrity of information is assured by protecting the history of communication from intentional, unauthorised or accidental changes (Clark and Wilson, 1987). In the interactions between parties this is exemplified by the trustee's record keeping and the correct maintenance of files that testify to the process of information disclosure and shared understanding. The integrity of such records, online, is attested to by the system or management processes and audit.

The principle of the availability of information ensures that trust forming information is accessible and is not subject to service denial as a result of the inadequate provision of security controls or due to the loss of service in a disaster situation. In the case of availability loss the services cannot be accessed to perform fiduciary duties.

Non-repudiation is a security mechanism by which evidence is maintained so that both sender and recipient cannot deny having participated in the communication (Tipton et al., 2006). This is assured by non-repudiation of origin and non-repudiation of receipt. In offline situations this is assured by requiring signatures to verify the intention, presence, knowledge and identity of the parties (Casaló, Flavián and Guinalíu, 2007). Online non-repudiation is assured by the use of digital signatures and use of contracts and is used to attest to the informational principle of consent to contract and the acceptance of the terms and conditions.

Although the basis of behavioural trust in electronic environments is rooted in consumers' belief in the security, dependability, and competence of the systems that they interacting with under conditions of potential risk (Kini and Choobineh, 1998), the consumer must also trust the transaction medium (Lee and Turban,2001).

It can be inferred that confidence in trustworthiness signals passed to trustors online is the subjective probability with which consumers believe that their personal information (private and monetary) will not be viewed, stored, and manipulated during transit and storage by inappropriate parties in a manner inconsistent with their confident expectations (Casaló, Flavián and Guinalíu, 2007). Therefore, the protective measures afforded by the C-I-A triad of controls is crucial in initiating the flow of information that passes between parties in a trusting relationship.

2.20.2 Identity

Identity is important during trust formation in the physical world because it ensures that the passing of signals between parties who are acquainted with each other (Donath, 2007). The power of identity in the physical domain lies in each party "knowing" who the other person is, and the power of "seeing is believing" or veridicality (de Marneffe et al., 2012). In the physical world, where trust is not a universal relationship between all parties, identification is a means of differentiating trusted entities from other, untrusted, parties. In contrast, online identities and choices are different because in identity domains, participants avoided options

preferred by majorities and abandoned preferences shared with majorities. Individuals diverge, in part, to avoid communicating undesired identities (Berger and Heath, 2007). That is, in online situations the identity presented by a participant may not be congruent with their real world attributes.

For trustees, a face-to-face meeting is a way in which to verify who a potential trustor is, to discuss their expected outcomes and allow them to disclose their vulnerability situation. In return, the trustor can evaluate the abilities, motivations and benevolence of a potential trustee. Building trust involves building relationships and face to face meetings, at which the credentials of the trustee (birth certificate, passport) are provided as evidence of identity serves both parties in verifying who is accessing services, anchoring the provided details to the person in the branch. During identity verification, the polarity of trustworthiness evaluation is reversed, as the trustee seeks to carry out trustworthiness checks on the trustor to ensure that the resources the trustee commits to the relationship are potentially covered. The trustor becomes aware of the risks taken and motivation for the trustee in helping them achieve their goal. Face-to-face meetings provide a simple mechanism to detect the truth of claims and of value congruence. It also assists in confirming the bi-directionality of trust and affirms the power status of the parties.

When building new trust relationships the information signals passed between strangers are carried out in an environment that is separate to the channel through which the transactions take place. Oftentimes, service providers such as solicitors or doctors will offer free introductory consultations so that this exchange of information

happens. Trustees have a duty of care to their beneficiaries when carrying out their fiduciary duties that perform the dual functions of controlling discretion and maintaining business integrity (Mitchell, 1990) and the precursor to trust formation is knowing who it is that is being trusted and for what (Blois, 1999).

Allied to the verification of identity of a party is the concept of identification with the other. Identification is a means by which points of view are matched through a relationship allows the adoption of both viewpoints and allows parties view the world through a different social reality that promotes mutual understanding (Cohen, 2001). This is the basis for evaluating the integrity and values of the trustee for trustors, and is used by trustees as a way to evaluate and accommodate the trusting attitude stance of trustors by sharing mutual goals and intentions. The precursors to behavioural trust differentiate individuals by identity from the 'generalised' other community identity (Mead, 1934). Being able to identify individuals is one way in which social capital effects can be realised (Fukuyama, 1995). As trust is essential for relationship development, it teaches individuals more about themselves, and by learning to trust individuals can feel more self-confident (Mietzner and Li-Wen, 2005). This formation of identification-based trust can materialise when each party has internalised the other's preferences, so that one party may serve as the other's agent, with the other being confident that their interests will be fully protected (Shapiro et al., 1992).

In seeking to form trust relationships beyond transactional interactions electronic environments lack a single coordinated channel with which to verify identity in the pre-delegation phase and the lack of affective contact between parties

means that online relationships may have difficulty progressing beyond a calculative basis. This is because familiarity is influential in the assessment of perceived reputation of a potential trustee (Van der Heijden et al., 2003). The role of affective trust in verifying identity in real world situations is replaced as a top down facilitator of trust with the bottom up approach of online cognitive trust mechanisms. Confirming trust in online identity through multiple authentication factors (Huang et al., 2014) endeavours to balance the personal psychological foundation with the calculative and cognitive elements of behaviours.

The management of the relationship boundaries and context of trusting behaviour is managed through privacy, which is discussed in the next sub section.

2.20.3 Privacy

Privacy relates to the amount of control over personal information that a party has over the disclosure and dissemination of personal information. Privacy can be viewed as a process of boundary regulation, controlling how much ,or how little, contact an individual maintains with others (Derlaga and Chaikin, 1977). Controlling the boundaries of an interaction allows the trust context to be maintained and separated from concerns other than the matter at hand, and helps to maintain the scope of the trusting relationship.

The reasons for seeking privacy can be further classified into two themes of control over intrusion and control over disclosure. Control over intrusion includes the

avoidance of behavioural response from others; avoidance of embarrassment; and the avoidance of evaluations by others. Control over disclosure includes the protection of enjoyment; protection of information about the self; protection of the self-image; and protection of the undesired self (Goodwin, 1991). Privacy places the individual at the heart of what they choose to disclose about themselves and the concept of communication context involves the amount of information an individual is willing to offer. In low-context cultures, individuals provide little information, while in high-context cultures, individuals volunteer background details and other related information (Im et al., 2011).

Generating an environment of privacy disclosure safety is seen in the real world whereby trustors will often conduct business in private spaces away from the transactional side of the business interaction, for example in the solicitors' or bank managers' office. In addition to the verification of identification, a private environment allows the boundaries of vulnerability disclosure to happen in an atmosphere where the interaction is solely the two parties to the trust relationship and encourages 'truth telling' (Fisman and Khanna, 1998). The giving of reasons connects people with one another, is of normative importance, and the giving of reasons always says something about the relation itself (Tilley, 2004). By evaluating reasons as motivators people are 'moved' to do things, from intention to behaviour. The passing of reasons fosters interpersonal trust and allows the parties to create a relationship away from the information turbulence of the trustees' business.

It is also important to recognize that not all individuals perceive privacy similarly, because privacy is highly contextual (Malhotra et al., 2004; Schoeman, 1984). Privacy is important to the trustor in setting the boundaries for disclosure and how they maintain social distance in different contexts by keeping secret or sharing their personal details. Inappropriate privacy disclosure by trustees in trust relationships can destroy the bond as *"Trust is a fragile plant, which may not endure inspection of its roots, even when they were, before the inspection, quite healthy"* (Baier, 1986: 260), and in the destruction of trust betrayal is not due to the failure of trust, but to failure of trustworthiness (Hardin, 2002). In guarding the relationship forming space it is incumbent upon the trustee to maintain the privacy of information exchanges to ensure the boundaries of the trusting environment. At an organisational level it is likely that the realisation of the trust bond involves the participation of other trusted parties in the fulfilment of their duties (Schoorman et al., 2016). Therefore, authorisation security mechanisms should exist within trustee organisations to ensure that information is only shared with those others authorised to see such communications.

Contextual authorisation enables a certain operation to be carried out only after identity authentication, or if there are guarantees of the identity of the party one is dealing with. Authorisation is generated from authentication by applying mechanisms to ensure that they access only the information that is applicable to their role in the matter at hand. Thus, privacy is a form of 'contextual integrity' that ties adequate privacy protection to norms of specific contexts and ensuring that information

gathering and dissemination are appropriate to those norms that govern that particular context (Nissenbaum, 2004). Ensuring contextual integrity through information confidentiality is one way in which privacy can be guarded in online information space.

Privacy is important because inappropriate disclosure of private information relating to trusting relationships gives rise to feelings of betrayal that are registered when information is shared without the permission of the trustor. Although trust formation may be purely cognitive or calculative, the transformation of the cold reasoning of trusting partner choice can lead to the hot emotional fallout of betrayal due to the inappropriate exposure of trusted relationship information.

2.20.4 Environmental Factors Summary

The formation of trust relationships in electronic contexts necessitates the provision of trusting spaces that protect the identity, privacy and security of risk taking parties. The provision of these controls are afforded at interpersonal, organisational and institutional levels.

Identity is a fundamental dimension in building relationships and validating the identity of a participant allows access to services that are provided through the multiple factor security controls of authorisation and authentication. Identity passing information is also essential for payment (Kolsaker and Payne, 2002), and this is an area where the compromise of security when combined with identity can cause feelings of betrayal through inappropriate disclosure and theft of identity credentials

(Berger and Heath, 2007). Privacy builds in the preferences of the individual by helping to define the boundaries of the relationship, and these boundaries are enforced by applying access mechanisms to the information exchanged in the relationship. Research into electronic commerce and trust has advanced the view that privacy and security concerns are experiential (Casaló, Flavián and Guinalíu, 2007; Loader and Walker, 2010), and that there is no conflict between the demands for both privacy and security within a trust relationship. Security may override the need for privacy, which is not always an automatic right in legal terms, and it has been shown that monitoring decreases citizenship behaviour whilst increasing perceptions of fairness of treatment (Niehoff and Moorman, 1993). Therefore, it may be necessary to breach privacy on fiduciary duty or legal grounds, where security takes precedence or is enshrined in law, for example as part of money laundering regulation or where medical staff need to disclose gunshot wounds.

The relative importance of identity, privacy and security in a shared environment needs to be viewed from the perspective of the information passing between different private contexts in which the information relating to identity are verified and protected throughout processing to ensure that the security afforded by environments allay the feelings of vulnerability that are felt by consumers in trust situations. Fostering confidence in the structures that are in place to protect trust formation and trusting actions assist the process of fostering a confident belief in trustors that their vulnerabilities will be protected.

2.21 Risk Taking Relationships Conclusion

This section analysed the determination of decision and behavioural trust by outlining the processes of assessment by the trustor of how the expected outcomes and vulnerability reduction needs are met by the attributes of the trustee.

The confident beliefs of decision trust emergent from the assessment of trustworthiness are manifested into the delegation of all or part of the actions required to gain outcomes. Beliefs are transformed into a relationship through the intention to act involving goal setting and action with another party, or else acted on directly by trustors delegating action where the case for trust has not been made.

The risk taking relationship forming process is also dependent upon environment controls to protect trust spaces. The effect of security, identity, and privacy controls were explored, alongside an analysis of the interplay and influence they exert on the processes that are carried out within risk taking situations.

The action-realising process described in this chapter is predicated on the assertion that trustors take account of attitudes, social norms, and perceptions of behavioural control to form beliefs and intentions prior to taking action. The balance between these endogenous antecedent factors gives rise to the exogenous and observable reality of behaviour. Influencing factors and the hidden nature of the underlying constructs make the prediction of behaviour from its' antecedents, and vice versa, susceptible to both the fluctuations of the mediating construct variables as well as external moderating and confounding variables.

Trust can be seen to act as a complexity attenuator to reduce the risks involved in taking action to effect change, comprising of decision and behavioural trust. Decision trust is utilised to act as a selection attenuator to manage the complexity of choosing a trust partner, using the logic of possibility. Behavioural trust that is the manifestation of decision trust is also a risk attenuator by managing the complexity of risk inherent in actions, expressed using probability logic. Trust, therefore, is the original complexity management system that suggests the possibility of the probability of gaining a successful outcomes to reduce vulnerability and produce action.

This socio-technical trust system is not infallible and in terms of electronic environments the necessity to develop low-cost methods to reveal the reliability of participants is thus a crucial step in enabling trustworthy participants to perform and return a higher outcome to themselves and the discriminating trustors (Ostrom, 2014). The following section will look at the issues associated with using online systems to discriminate trustworthiness and the influence that information security has on the process.

2.22 Section Three: Relationships in Digital Contexts

Taking account of the conclusions from the previous section on risk taking relationships, it stands to reason that the inclusion of trust as part of a risk reduction strategy in any business should decrease processing costs as the presence of trust decreases the need to monitor other parties. Trusting relationships help to lubricate

transactions and assist the realisation of social capital. In common with other business activities such as transaction processing and order fulfilment, trusting relationships need to have an awareness of the security concerns specific to this type of environment, and the measures and controls necessary to ensure safety in exchanges.

This final part of the literature review starts with an analysis of the phenomenon of cybersecurity and continues by exploring the different types of environments where trust information is handled, the possible vectors of attack on these types of systems, and the controls that should be in place to deter these types of attack.

2.23 A Definition of Cybersecurity Management

The definition of the word 'cyber' in relation to the study of the security aspects of online environments is one on which there is little consensus. It has a variety of different meanings in different contexts, and the lack of common understanding often leads to misunderstandings and bad policy decisions (Futter, 2018).

The study of cybersecurity has roots in the conjunction of the fields of computing and security studies and many currently accepted definitions of cybersecurity relate to the protection of systems and ICT assets (von Solms, 2013). Practitioners in the field of cybersecurity management implement information security with reference to the C-I-A triad of controls, see Figure 2-2 and guidance (Disterer, 2013) to achieve compliance with published standards (ISO/IEC 27001, 2013; ISO/IEC 27002, 2013). However, it is clear that if the problem of information security was only concerned

with implementing formative controls to technology there would be no cybersecurity issues.

Information produced as part of the interaction between parties in trust formation should be considered a subset of a wider strategy because the data obtained in the exchanges reflects the relationship between parties as well as the mediating systems of communication. This focus on information, rather than the mode of communication and assets is what differentiates information security from the definition of cybersecurity. Information Security is hard to measure and quantify, and involves a myriad of risk, control and cost trade-offs when applied in practice. Therefore, considering information security as "*a well-informed sense of assurance or confidence that information risks and controls are in balance"* (Anderson, 2003) captures both the desirability and unobtainability of the ideal equilibrium.

In the case of exchanges between partners there are two targets of trust, the trustworthy entity providing the trust known as party trust and the mechanism through which it is provided, known as control trust (Gefen, 2008; Pavlou, 2003; Tan and Theon, 2000). However, the reality of online business extends beyond the trust shown in trading partners, as trusting also involves trust in *"the infrastructure and the underlying control mechanism (technology trust) which deals with transaction integrity, authentication, confidentiality, and non-repudiation."* (Ratnasingam et al., 2002: 386). Technology governs control trust through the mechanisms of integrity by maintaining the accuracy of information, using confidentiality as authentication to verify access to, and sharing of, service data, and using non-repudiation to ensure

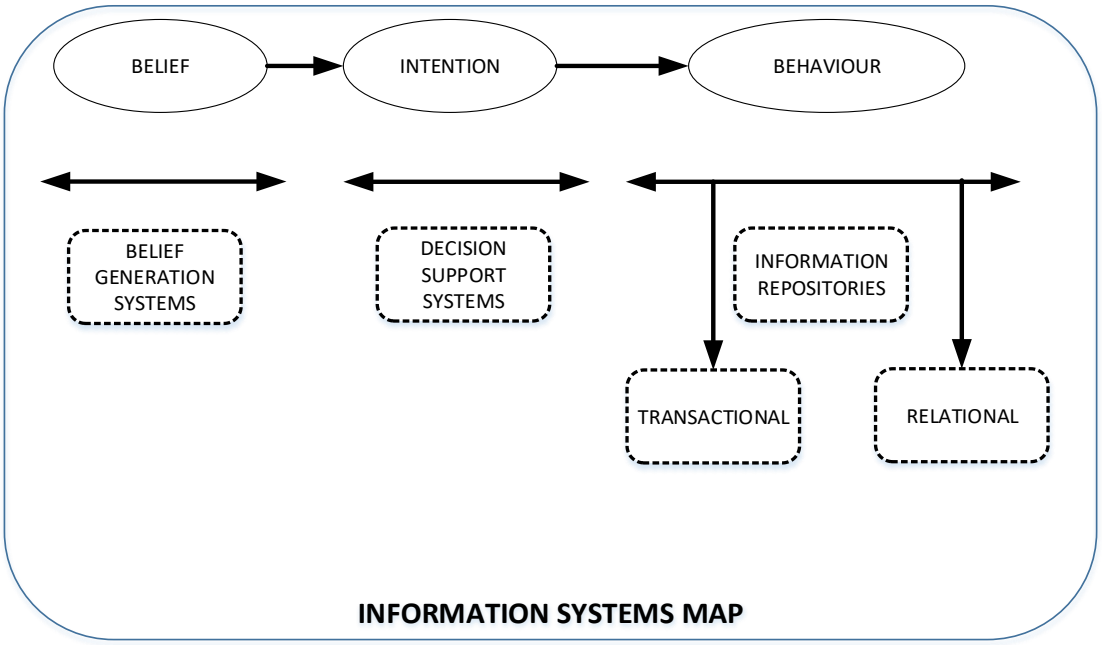
service consistency and the honouring of promises. This helps to ensure that *"the members of that system act according to and are secure in the expected futures constituted by the presence of each other or their symbolic representations"* (Lewis and Wiegert, 1985: 968)

A synthesis of the management and cybersecurity disciplines to produce the role of cybersecurity management used in this thesis is therefore:

"The management of information systems to ensure that the confident expectations of trust are met in online environments by the appropriate controls on transaction integrity, authentication, confidentiality, and non-repudiation."

The purpose of information systems with respect to trust is to protect the boundaries of the Risk Taking Relationship in the belief generation, decision taking and information storage stages of processing. An assessment of the protection required for trust in digital environments can only be made if the purpose of those information systems in supporting trust is mapped to the processes they support (Vishik and Balduccini, 2015). This ontological mapping is shown in Figure 2-4 and the types of trust support systems and the inferred potential for cyber-attack and the threat spaces are detailed in the sections that follow.

Figure 2-4 Mapping Information Systems to Trust Formation



INFORMATION SYSTEMS MAP

2.24 Belief Generation Systems

Belief generation or trustworthiness support systems are those systems that help to cross influence between the offline and online presence of trading entities. Organisations invest in high value online and offline expressions of trustworthiness and individuals rely on matching both the external representation of this trustworthiness with other information received from their social networks to reach decisions on who to trust. Offline investments have been shown to influence online relationship participation in all four areas of banking trust (Ha, 2004), where flow, structural assurance, perceived web site satisfaction, and perceived extent of future use of banking websites were positively correlated to banks' offline presence.

The complementarity of offline and online displays of trustworthiness are used to demonstrate the worth of being associated with trustees, and the trustworthiness presence is actively managed by organisations to evoke trusting beliefs in individuals.

2.24.1 Reputation Management

Reputation has been defined as the amount of trust inspired by a particular person in a specific setting or domain of interest (Marsh, 1994). Reputation is also a form of social control mechanism in which other participants can enforce societal norms on organisations to comply, face closing down, or improving their reputation.

The relational advantages of a good reputation include being able to charge a premium on goods or services, and being the recipient of important social capital (Abdul-Rahmen and Hailes, 2000). The advantages of being trusted also include increased levels of appreciation, an increase in the number of potential partners, and the prestige of becoming a sought after business partner (Castelfranchi, Falcone and Marzo, 2006). Selecting a partner with a good reputation simplifies the decision process for the trustor, so organisations seek ways to communicate their good reputation to others.

2.24.2 Social Media

Given the importance of reputation, it is not surprising that the influencing and controlling of an individual's or group's reputation is a high priority. However, social media is difficult to manage in advance, and the problems of organisations may be

revealed or exacerbated by the interactivity of content posted online. This raises a reputation risk for trustees (Aula, 2010). In modern environments it is not always possible to control either the message or the medium.

Social media engagement by companies includes improving the online presence of the trustee by improving the tagging and search engine optimization (SEO) of company-published materials, getting mentions of the business or individual on third-party sites that rank highly on search engines, producing online press releases for authoritative websites to promote brand presence.

2.24.3 Structural Assurance

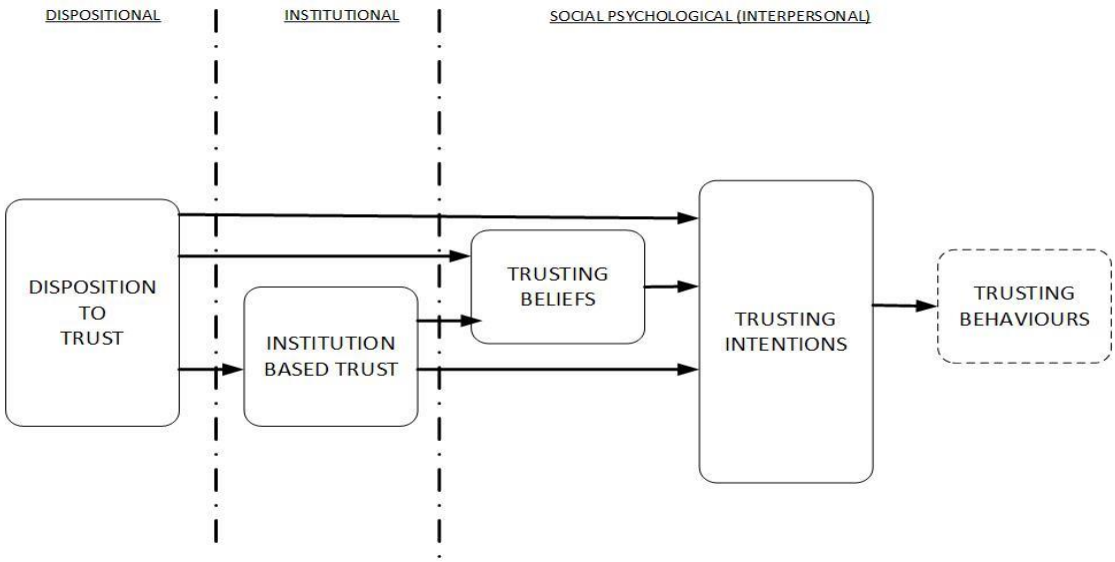
The moral imperative for trust in wider society can trace its' roots in the responsibilities and obligations on higher institutional power and the relationship with the individual as part of the social contract (Rousseau and May, 2002), delineated by the consent of the individual, agreement among moral agents, and a device or method by which an agreement, actual or hypothetical, is obtained (Dunfee et al., 1999). In consenting to relinquish some degree of freedom of action, individuals benefit from the security and protection such institutions provide.

Institutional safeguards are applied to all participants in the online environment through the standards and protocols adopted by the governing bodies (Choucri et al.,

2014). This enables the confidentiality of interactions, the integrity of the messages passed between parties and the availability of the infrastructure to enable interaction to happen. Implementing institutional security safeguards ensure structural assurances, defined as the belief that success is likely because such contextual conditions as promises, contracts, regulations, and guarantees are in place (McKnight et al., 1998) to positively influence the trusting decision, and institutions lend credence attributes to those organisations that they oversee. The role of institution based trust is a key mediator in the provision of security by supporting the beliefs and intentions of trustors online (McKnight and Chervany, 2000) and is shown in Figure 2-5. This model was further developed (McKnight et al., 2002) in the Web Trust Building Model whereby beliefs about vendor reputation, site quality and structural assurance combined to influence trusting intentions, with structural assurance also contributing to behavioural risk reduction.

Structural assurances come with societal concerns about surveillance, as evidenced by the NSA surveillance operations (Greenwald, 2014) are countered by the provision of institution backed controls and legislation to underpin transparency of institutions and confidence in the system to overcome risk in going beyond decision trust to behavioural trust.

Figure 2-5 McKnight and Chervany Trust Building Model



Due to the supra-national and collaborative nature of the internet the institutional provision of service is provided by governments, standards bodies (ICANN, IANA) and protocols (HTTPS) that give assurances to citizens that online engagement is safe. Institutional-based provenance is formed through societal institutions such as certification by a credible source or governmental regulations (Zucker, 1986). Critical services, including Domain name systems (DNS) and security protections for these zones (DNSSEC) utilise digital signing technology to provide certification proof verified by the operators of the website (Sample and Karamanian, 2015). This provides a form of infrastructure and application certification trust by providing that which is essential to a communication channel but cannot be transferred from a source to a destination using that channel (Gerck, 2002). Institutional control mechanisms provide the engineering and provenance schemas of interaction that ensure that the online environment can support the verification and validation of merchants, and assurance via the protocols that protect sensitive information exchange online.

By legally protecting customers from economic losses during a transaction or by raising the trust levels in carrying out transactions it is possible to use controls as a substitute for trust. The application of unauthorised credit card loss protection for trustors and the widespread usage of trusted third parties like PayPal or WorldPay in processing payments acts as a substitutional relation used on behalf of trustees to protect trustors in online environments. The use of such payment services and guarantees offers a uniform social indicator to give assurances of trustworthiness.

2.24.4 Cyberattack Vectors

Organisations and individuals invest time and resources into relationships with each other (Morgan and Hunt, 1994). The presence of relational capital is crucially based on beliefs, and is a form of capital that can be manipulated by manipulating beliefs (Falcone and Castelfranchi, 2008).

The manipulation of belief can take several forms. Amplifying negative sentiment aims to call into question the trustworthiness of the trustee; inconvenient information about past interactions; by introducing uncertainty; or through breaking the bond that exists between companies and their governing bodies. Alternatively, organisations can make other parties dependent on them by making the other lack resource or skill; inducing in the other a given goal, need or desire in which the other party is not autonomous; and by signalling the presence of skills and resources to others (Castelfranchi et al., 2006).

Inconsistent communication behaviour can lead to a sense of disruption in the attachment between parties by breaking the cognitive schema of interaction (Tesser, 1977; Bowlby, 2012), disrupting the sense of situational normality (McKnight et al., 1998) and causing psychological insecurity (Mikulincer, 2003). This means that the customer can no longer rely on the word of the trustee because it is delivered in an unreliable fashion, or by an inconsistent use of different media by using a different interaction medium. Messages become confused and trustors can fall prey to phishing attacks, scams and confidence tricks. This loss of reliability can lead to communication channel disruptions. Consistent with trust research, customers may be more forgiving where the cyber-attack could not be foreseen, or be more patient with situations where services struggle to cope, as seen in the 2017 NHS WannaCry encryption attack. (Graham, 2017).

It is uncertainty in the communication signals received that introduces reputation risks for organisations and commitment wariness in trustors.

2.24.5 Belief Generation Systems Summary

A major advantage of digital environments is the ability for service providing organisations to communicate their brand and values to the widest possible audience to trigger the tendency towards knowledge structures that produce belief in consumers. Organisations enhance and protect their brands and the trust that they evoke by implementing security strategies to protect them. As security is a usability belief that is stronger than usefulness or ease of navigation (Salisbury et al., 2001),

privacy is a proxy indicator of the discretion required to apply trust (Ha, 2004) and information quality directs message relevance and monetary benefit (Krishnamurthy, 2001) the potential benefits of secured belief information outweigh the costs of implementing the security controls.

Online reputation relies very heavily on the transmission and interpretation of information, and therefore protecting this information from impersonation or criticism is a priority for many organisations with a digital presence. Control mechanisms are also designed to detect or prevent opportunistic behaviour and errors by institutional reliance rather than trust, enhancing the integrity and reputation of the trusted party. Although it is not possible to create trust just by having a counter-party or a control procedure (Tan and Theon, 2000), the trustor has to be convinced of the quality of the source, backed by the assurance of authenticity, reliability and adherence to standards conferred by institutions.

Belief generation and trust formation promotes the making of delegated decisions towards preferred attributes, features and suppliers of services (Roy et al., 2019). The systems and their protection is considered in the following sub sections.

2.25 Decision Support Systems

Customer decision systems are those that add value to the decision making process based on the communication of trustworthy information. The value of these systems for the individual lies in the improved decision making elements offering expanded and enhanced cognitive choices (Falcone and Castelfranchi, 2001). Through

system mediated interaction the communicatively-oriented trustor makes efficiencies in choice and delegation decision making. In turn, the value of being a 'trusted trustor' helps to mobilise the reputational resources of the organisation in terms of loyalty and access to services as reward (Ball et al., 2004).

2.25.1 Searching and Browsing

Browsing for information online allows choices to be evaluated and compared. The attributes that customers look for in products and services can be classified as being search, experience and credence (Darby and Karni, 1973). Search attributes are those that can be verified before purchase, experience attributes can only be verified after the purchase or use of the product, and credence attributes are those that are difficult to verify even after the product or service has been used.

Expanded search options online allow simple criteria to return rich search content that incorporates offline cues to trustworthy services. As an example, brand names are considered to be valuable assets that help communicate quality and evoke specific knowledge structures associated with the brand (Srinivasan and Till, 2002; Keller, 1993). Experience attributes can be inferred from feedback scores can be used and where they are based on the aggregated transactions of others the earned reputation reflects stakeholders' overall evaluation of a company over time (Gotsi and Wilson, 2001). Credence attributes of potential trustees is more difficult to communicate and evaluate objectively, with trustees drawing attention to their history of reliability, the future focused efforts of new market entrants, and the

professional accreditations and credentials of their practitioners. These investments represent sunk costs that are not easily retrievable or recoupable by the holders of such evidence. Reputation transfer and the generalisability of reputation from offline to online are critical factors in evaluating the credence of trustees (Riegelsberger and Sasse, 2001). These investments are used as strategic assets that are indicative of the ability to mobilise the organisations resources (Amit and Schoemaker, 1993).

Support systems are used by consumers in the most part to guide decisions on how to, who to, when to, and what to delegate. In many cases the information required is incomplete (Simon, 1972), so rationality is bounded because the information required to make fully informed delegation decisions is not present. When there is no time to collect all the required variables about delegation the presence of the search, information brokerage and recommendation systems provide the heuristics to ease the cognitive load on individuals. These services are analysed in the following section.

2.25.2 Brokers and Intermediaries

Use of a trusted or independent third party allows customers to signal vulnerability or communicate a need or requirement without exposing themselves to the security and privacy risks of broadcasting the requirements online. Third parties approach the providers of services on behalf of customers, optionally checking the integrity of trustees and running price or suitability matching algorithms to indicate which service providers match the requirement (Sarker et al., 1998). Broker services

help to ease the load of cognitively or domain naive customers by their ability to lower the cost of information production (Ramakrishnan and Thakor, 1984), and present the results of pre-screened searches to the client.

Information brokers may also act as intermediaries, providing a market infrastructure and a community of sellers acting within the marketplace. Intermediaries (Pavlou and Gefen, 2004) provide institutional protections offered under a well-known brand and add the value of domain knowledge in knowing the kinds of questions to ask of products, the kinds of features and feedback that other customers provided thus brokering between the interpersonal level of trust and the organisational level of trust. (Hong and Cho, 2011). Direct recommendation based on experience, or on the information provided from search services and intermediaries may be made available via recommender systems, and the characteristics of these are analysed in the next sub section.

2.25.3 Recommender Systems

Recommender systems are software tools and techniques that provide suggestions for items that are most likely of interest to a particular user (Ricci et al., 2015). Referral and recommendation by other customers (Jøsang et al., 2007), or as determined by patterns of previous interactions (Shao et al., 2009). Advertisers may compete in auctions to place preferred content in online results pages, or use targeted advertising where the content of previous searches is known (McMahon et al., 2013).

The usefulness of recommendation systems is dependent in part on the novelty or interestingness of the information presented measured in terms of information entropy (Shao et al., 2009). The relevance of recommendation as a suggestion may be welcomed as an insight or dismissed as an intrusive infringement of privacy (Zhu and Chang, 2016). Good recommendations provide important social enhancement for trust due to using social networks as a proxy for emotional support and engagement (Lewis and Wiegert, 1985) and assist consumers in verifying the experience attributes of products and services.

Acting on recommendation also depends upon the due diligence of the customer receiving the recommendation to filter the results based on their personal attitude and their assessment of the source (Nurse et al., 2011). Trustee recommendations are based on either first or second hand reputation information or information on other participating nodes in the recommenders' network or as a substitute for direct observation (Jøsang, 2007; Panchanathan and Boyd, 2003), and as such the reputation of the recommender is also an important consideration.

Counter to this, many web based feedback scores assign a single recommendation value without history or context. This raises questions about the value labels recommenders place on social connections (Golbeck and Hendler, 2006), and the source trustworthiness of recommenders is required to discount the effects of untrustworthy peers acting maliciously (Xiong and Liu, 2003).

2.25.4 Cyberattack Vectors

The gaming of decision support and recommendation systems can circumvent the sunk costs of trustworthiness, and are exemplified by bad mouthing attacks, on-off attacks, newcomer attacks and Sybil attacks (Sun et al., 2008). A Sybil attack is where a number of multiple identities are forged, acting under the supervision of a single entity (Douceur, 2002). Organisations can arrange creating fake positive reviews to counteract negative ones, or proactively offer free products to prominent reviewers (Wikihow.com, 2018). Subtle manipulation in the influencing of decision support systems undermines effective and efficient mechanisms for overcoming information asymmetry between online sellers and buyers (Malbon, 2013). Non-disclosure of sponsorship (Nekmat and Gower, 2012), and highlighting positive customer testimonials to outperform negative results in a search is not unknown (Engler et al., 2015). The presence of poor customer reviews or the deliberate masking of information harmful to the reputation to organisations or products reduces the perceived integrity and trustworthiness of organisations.

Decision support system integrity is challenged when the systems involved are rigged or gamed to encourage to make different choice intentions based on the biased information.

2.25.5 Decision Support Systems Summary

Decision support systems in digital environments seek to guide consumers towards trusting relationships by providing information that is used to assess the

search, experience and credence attributes that trustees possess. This allows them to evaluate the attributes that are congruent with their values and beliefs. In turn, this influences the decision intentions that underlie the delegation of tasks to another party. Attacks on this type of information system are those that skew the integrity of attribute review by introducing information into the context of decision making. This has the effect of hindering reasoned assessment of how the trustees fulfil the obligations to the trusting relationship, and call into question whether it is correct to place trust in the service provider.

Where customers choose to delegate action to trustee organisations, behavioural and action output information is stored in information systems that are used by those organisations to manage the relationship between trustors and trustees, and the role and nature of these are examined in the next sub section.

2.26 Information Repositories

Action generates information, and when the action is delegated, the information produced becomes the property of the causal agent, who is in receipt of a better signal than the principal (Levitt and Syverson, 2008). Organisations as the owners of agents collect a great deal of information on participants, including identity and service tokens as well as their website behaviour, browsing and purchasing habits. Delegated task behaviour produces data that can be used to understand and communicate more effectively with the customer. Where the relationship is a trusted one, communication can include feeding back to the trustor via portals, targeted advertising, or using the

preferred relational status to communicate offerings and signal pre-play information when providing services. Trust information is also used to refer details on to other parties. The information generated by customer trust increases the trustees' understanding of the domain and data sharing with trusted third parties can lead to efficiencies in organisation decision making, process improvement and service offerings through agency mitigation (Chami and Fullenkamp, 2002).

The effectiveness of trust repositories in making these improvements lies in the importance of the integrity of information that is stored about customer vulnerabilities, preferences, motivations and interactions. Restricting the audience by information confidentiality ensures that the data is appropriately shared whilst privacy respect maintains the contextual integrity of the relationship (Barth et al., 2006). The availability of these repositories are maintained to ensure they correspond to the C-I-A principles (Figure 2-3 The C-I-A Triangle).

The information management systems used to further the relationship beyond the first transaction is analysed in this section. These systems are designed to nurture the transactional relationship into a fuller, richer relational one.

2.26.1 Relationship Management

Relationship management covers many types of information systems that are used to manage organisational information. These include sales management systems, supply chain management systems, and customer relationship management. Relationship management involves not only the management of tasks associated with

accounts, but covers the wider trust relationship in general, the contact lines and ties that influence the effects of personal engagement, pricing and the history of interaction.

Modern CRM tools incorporate offline and online lines of information that seek to understand customers through the use of people, processes and technology, with the aim of building customer relationships and relationship development (Chen and Popovich, 2003). The role of the relationship in marketing products can be divided into those companies focused on transaction volumes and those whose interests lie in developing the relationship (Dibb and Meadows, 2001). As such, the information contained within them may be sensitive, subjective, contextual, or personal. In the case of electronic health records systems, privacy concerns may be one of the major barriers to wider adoption (Hillestad et al., 2005).

As the integrity of data used in decision making is important organisations may use Master Data Management systems to ease the administrative task of updating and merging records of differing types to integrate disparate customer information into cleansed and standardised 'true' records. Master data records typically are used many times but do not change frequently (Haug, 2011). They frequently contain the most sensitive personal data held in record systems, and the details contained within them are used as templates in the creation of transaction records.

Master and transaction records are stored in archives and systems by loading additional records into databases, files, or business intelligence (BI) systems to support organisational decision making based on longitudinal trends. Many systems

rely on multiple signal processing whereby different information sources are joined using identity credentials to build a profile of individuals and to train statistical models (Joachims, 2002). The large stores of data that are generated by interactions with trustors may be utilised to infer data structures and relationships (Weiss and Provost, 2003). In this way, they generate new master data based on inductive observations of transactional data.

2.26.2 Machine Learning (ML) and Artificial Intelligence (AI)

Machine Learning is based on data as inputs to statistical models that are used to generate recommendation, give expert insight or diagnosis and generate added value services (Witten et al., 2016). Artificial Intelligence is related to Machine Learning but mimics the logical cognitive modelling of humans to pattern detection and problem solving (Conte and Castelfranchi, 2016) using technologies and statistical techniques to synthesise the models used by Machine Learning into supportive analysis and action, which may impact social choice. (Goldsmith and Junker, 2008). The inclusion of ML and AI systems in this analysis of information repositories serves to highlight the potential confidentiality and integrity risks associated with post collection processing of behavioural indicators.

ML and AI rely on logical, cognitive processing over the holistic signal processing used by humans (Newell and Simon, 1972) and face the constraints of using historical training data to predict future events and not taking into account situations and contexts on which to base the analyses (McCarthy and Hayes, 1981). Predictive

systems do not yet fully take into account the subjective, holistic decision making of humans in engaging in trust relationships to affect change. New trusting relationships may presage a step change in behaviour on the part of individuals, who are not always constrained by algorithmic habituation of the past.

Using ML and AI systems to predict behaviour relies on assumptions being made about individuals, their intentions and environment. As such, they present opportunities to develop the relationship with individuals. However, incorrect assumptions and algorithmic actions taken by such systems can lead to bias in decision making that can disadvantage individuals or groups, and may utilise out of context data (Osoba and Welser, 2017). This leads to integrity and confidentiality (disclosure) concerns that can be used in cyberattacks.

2.26.3 Cyberattack Vectors

The presence of large amounts of sensitive data presents a risk that the confidentiality and privacy of information could be compromised by data breach, and this is a major focus of the efforts of organisations in their protections of such systems.

When the online and offline identity of participants becomes anchored authorised parties may be able to infer additional information about participants, which presents integrity risks where the calculated attributes are incorrect. An online relationship can be anchored through a number of master data attributes including institutions, residence, email addresses or usernames. The level of anchorage varies depending on the degrees to which online partners are identifiable and locatable

offline (Zhao et al., 2008). Anchoring online identities to offline persons can have both positive effects when used to provide personalised information products but can also have negative side effects. Joining different data sources to build a richer picture of individuals is common in user tracking using cookies, machine learning, business intelligence and artificial intelligence systems but presents risks where the profiling produces new data that reveals attributes about individuals that they have not offered, are not aware of, or that may be incorrect.

Mining data across contexts allows detailed cross-contextual profiles to be built up by external parties based on correct or incorrect data inference. Data mining can compromise privacy from correct usage, for example, Target retail correctly profiled a pregnant teenager before she told her family (Hill, 2012). Inappropriate disclosure can also happen as a result of prior data breaches, for example, the Australian blood donors data breach that revealed personal information disclosed to health staff (ABC, 2016). Advanced analytics systems that use Machine Learning or Artificial Intelligence are also vulnerable to training data poisoning attacks (Steinhardt et al., 2017), or may become biased where the quality and integrity of the input data is insufficient or where biased inputs to statistical models resulted in biased outputs that discriminate against certain groups (Russell et al., 2015).

Anchoring an online identity to Personally Identifiable Information (PII) such as birth date, address, social security numbers and bank details allows the authorised individual to access services and make transactions. Trust repository information can contain to the tokens that the customer uses to access multiple systems and agents,

and the unauthorised release of such information is potentially destabilising across platforms, as the persistent data that has been stolen allows potential attackers to build a profile of the customer using the same techniques used by organisations for use in phishing attacks or to compromise unrelated systems. Compromising the privacy of online identities associated with such information can allow other parties to authorise transactions and can lead to identity theft, monetary loss and blackmail (Jakobsson and Myers, 2006).

The consequences of trusted information repository breaches can be severe and remediation is costly. After a well-publicised data breach in 2015, communications company Talk, Talk saw 100,000 of 4 million customers leave the service resulting in costs in excess of £40 million, fines of £400,000 and implementing remedial security improvements including customer data handling, two factor authentication and a simplification of the product offering (BBC [2], 2019). When compromised, individuals experience not only a data breach but also a psychological contract breach (Robinson and Rousseau, 1994). In reasoning that they are being treated unfairly in social exchange terms they lose trust in the organisation, and seek to disengage and dis-identify from the group, for example by withholding data or permissions, using fake credentials and not engaging in citizenship behaviour (Restubog et al., 2008).

Cyberattack vectors concentrated on information repositories present risks to trust relationships because of the presence of anchored data. The risks include theft of the information; fraud, using services without authorisation; inappropriate disclosure through the failure of privacy safeguards when processing; producing

blended tracking profiles without context; and the creation of biased processing due to the poisoning of training data for ML and AI systems.

2.26.4 Information Repositories Summary

Trust repositories utilise transactional data to inform the delivery, promotion and production of services by leveraging the data points of transactions into information and insight though analytics. These longitudinal information stores provide information, not only on customer attributes and behaviour, but also generate records that can be used to attest to the trustworthiness and reputational characteristics of the organisation.

An exploration of the role of trustworthiness communication systems that aim to generate belief in trusting parties is explored in the next section.

2.27 System Controls

Trust formation processes in traditional face-to-face environments place emphasis during trust formation on the interpersonal processes involved in the following areas:

- Assuring the provenance of the trustworthy credentials of trustees.
- Verifying identity to access services.
- Ensuring that the boundaries of the relationship are preserved through confidentiality of disclosure to authorised third parties only.

- Affording communication secrecy to promote truth telling and vulnerability disclosure.

For customers, the provision of security is a feeling or a subjective mental state and is determined by the acceptability of the security measures as determined by the intrusiveness, effectiveness, threat level and demographics (Sanquist et al., 2008). This feeling of security is enhanced by the controls that are used to protect the relationship participants during the trust forming process.

2.27.1 Reputation Controls

In business to customer interaction the formation of a trust relationship allows the exchange of information between the parties. The resulting increased information entropy (Shannon, 2001) provides greater relational information exchange in which customers communicate the meaning of the information, whilst the trustee builds understanding of the customer habits and behaviour. Information exchanges build a store of 'relational capital' between the parties that is the result of investment and can be accumulated to be invested or further utilised (Castelfranchi, Falcone and Marzo, 2006). Individuals with common goals tend to perceive each other positively and organisations can be perceived as trustworthy and reliable because of their actions or because they are a member of a competent group. Therefore, a good reputation leads to trusting beliefs about an individual regardless of any first-hand knowledge (McKnight et al., 1998), building party trust.

To maintain a trustworthy image, organisations will often signal their adherence to policies on privacy, information usage, storage, and destruction (Malhotra et al., 2004). In online environments participants only perceive the control strength of security through advertisements and publicised information (Suh and Han, 2003) so wary trustors will seek to verify the published information with multiple external sources. As the recipient of the trust investment from the trustor should endeavour to ensure the confidentiality of information and exchanges to maintain the contextual integrity of interactions as part of maintaining their reputation.

2.27.2 Trustor Controls

The issue of identity is critical to people's source of meaning and experience. People make a distinction between their personal and social identities and a process of individuation is used by people to construct identity (Giddens, 1991; Tajfal and Turner, 1986). Identity is internalised and used to construct meaning, and in doing so helps to identify the roles and functions of the actor, framed by the primary identity of the individual, and in seeking trust actors fulfil the social roles of trustor and trustee to form a relationship. The packaging and editing of the self to make favourable impressions upon others is an essential and ubiquitous component of social interaction (Goffman, 1978) and the selective self-presentation aided by the asynchronous nature of many online interactions means that the identities that individuals construct cannot always be trusted (Hancock, Toma and Ellison, 2007).

Showing vulnerability in networked environments is perceived to be a risk activity, but without self-disclosure the opportunity of trust relationships cannot be formed. Self-disclosure varies according to the breadth or the amount of information disclosed; depth or the intimacy of that information and duration or the amount of time spent disclosing. In terms of the depth of disclosure, they argue that disclosed information can reveal either peripheral, intermediate, and core layers of the self. The peripheral layer is concerned with biographic data, the intermediate layer deals with attitudes and opinions and the core layer with personal beliefs, needs, fears, and values (Joinson et al., 2008; Altman and Taylor, 1973). As belief based disclosure about needs, fears and values used to construct meaning, trust formation requires disclosure of the self at a core level. Rather than choosing to display such core personal vulnerabilities trustors may choose to disclose information through the social veil of pseudonyms or third party proxy identities.

The risk for trustors is not in communicating, but in the content of that communication which can be used to associate the identity of the trustor with the information about their perceived weakness. In addition to the risk of inappropriate disclosure trustors also risk of loss of privacy associated with surrendering, intentionally or involuntarily, personal information and delegation of authority (Pavlou, 2003) to third parties to carry out processing on the information that is provided. Therefore, it is incumbent upon the trustee to protect the personally identifiable data of individuals that has been used to provide a service, and to maintain the boundaries of the scope of information that is required to provide such a service.

2.27.3 Relationship Controls

Agency Theory (Eisenhardt, 1989; Jensen and Meckling, 1976) considers exchange between parties within the context of a contract situation. Customers or creditors are the principals in the relationship, and trustees have ownership of the agents (Pratt, 1991: 2). By controlling the actions of an agent contracts and policy can be used to mitigate some of the problems and co-ordination issues associated with contracting and delegation.

In seeking to control the freedom of the delegated agent in it is necessary to consider the control of up to five classes of authority to the delegated party (Grandison and Sloman, 2003; Jøsang et al., 2007). These are:

- Provision, the trust that exists between the user of a service or resource and the provider of that resource.
- Access, the trust that exists between the owner of a resource and those that are accessing those resources
- Delegation, the trust that exists between an individual who delegates responsibility for some action or decision and the individual to whom that action or decision is delegated
- Identity that an individual is who they claim to be.
- Context that an individual has in existence of sufficient infrastructure to support whatever activities that individual is engaged in.

Delegation is a widely used mechanism for risk sharing that is employed in the fulfilment of tasks, but is also associated with the problems and risks of agency in passing the responsibility of tasks to others, either entrusted employees or automated systems. Therefore, in an environment of delegation is not an option, maintaining the relationship between parties is dependent upon controlling access and delegation rights to information used by employees, third parties, data processors, supply chain partners and other agents.

2.27.4 System Controls Summary

To protect the risk taking relationship online requires that actions are undertaken by trustees to ensure the safety of the relationship participants. Trustees can provide reputation assurance by creating and adhering to policies on the storage and processing of trustor relational information, by placing controls on the sharing and redistribution of information to third parties to retain the confidentiality and context sensitivity of the data, and by putting in place measures to protect the personal identity information and by requiring minimal amounts of that data to provide services to the trustor.

2.28 Digital Contexts Summary

There is a paradox between the need to trust and change (which involves the acceptance of risk) and the need to control change. Controls and protections of the trust formation processes need to balance the two perspectives. The inflexibility of

security may lead to the impression of change blocking, and security becomes a brittle defence that is circumvented by users.

The protection of context afforded by strong privacy controls can prevent the benefits of data sharing for research and recommendation or conversely the absence of such controls can lead to insecurity and mistrust from customers and a loss of reputation for organisations. From an agency point of view the tension between the risk averse agents of structure is confounded by the risk neutral transactional behaviours of customers. Individuals may be risk neutral in transactions, but are wary of identity disclosure online because it is the key to services in many different contexts.

Trust is an attractive vector for cyberattack but also offers a defence. It is a way to provide a measure of certainty that is not wholly conveyed by, or dependent upon, the online medium in which the interaction takes place. It provides a binding between structure and agents, part interpersonal relationship and part structured interaction. As such, it becomes a qualified reliance on information to counteract the unknowability of delegated actions in search of goals (Gerck, 2002).

Security for trusting parties in a shared electronic environment is necessary and begins with the need to protect the secrecy of signals between trusting parties that need to display vulnerability and the trustees who interact with them. This requires that security controls are implemented to protect the reputation of organisations, the relationship between parties, and the anchored identities of individuals.

At institutional level, protection is about ensuring the correct delivery of information messages and this level of protection is offered to all participants online through the co-ordinated efforts of governments and governing bodies, and by applying standards to message routing and delivery. At party level, confidentiality protection must be maintained between trusting parties to avoid disclosure of the discussions between them. At individual level, to access services or make payments it is necessary to anchor online trustors with their offline identity and associate this with sensitive personally identifiable information. Protection levels should be enveloped, to ensure that the lowest and most sensitive level of information, that of anchored identity information is not disclosed by applying the protection of secrecy to communicating sensitive information, applying access and authentication controls to information stores, and applying information privacy policies to guard contextual integrity.

2.29 Literature Review Conclusion

Critical analysis of the academic literature was conducted in a logical, narrative structure, looking first at the phenomenon of trust. This included a definition based on a meta-analysis of the prior work. The resulting definition of trust as positive expectation of behaviour where the trustee is willing to be vulnerable to the actions of another party irrespective of any ability to control that party forms the foundation of this research enquiry. This generalised definition was further explored by analysing the types of manifest trust, and the outcomes of trusting behaviour.

The complementary variable of trustworthiness was also explored. Trustworthiness was critically evaluated as a multidimensional variable, with the key dimensions of ability, integrity and benevolence which trustees signal to potential trustors through reputation. This lends a degree of complexity reduction and predictability of action that the trusting party measures against their trust expectations.

Further analysis into the formation of risk-taking relationships involving trusting parties examined the processes involved in taking action based on an evaluation of the antecedent processes and psychological states involved in belief formation. This was important because, if trust is a positive belief in the actions of another, then the bases of the belief are critical in intention building and taking action. An examination of the environmental conditions under which these psychological states are formed led to evaluation of the C-I-A characteristics of the electronic systems involved in evaluating the reputational characteristics of other parties used to support the formation of trust relationships in the digital space.

Trusting relationships act as a pathway between uncertainty and reliance and *'acts as a bridge'* to overcome missing information (Luhmann, 2018). This bridging role is especially relevant when communication is mediated by, computer system. The missing dimension of trust in electronic environments, namely interpersonal presence, therefore heightens the psychologically perceived levels of risk in electronic environments.

Cybersecurity concerns affect the antecedent trust generation mechanisms of trustworthiness and the outcomes of trusted communication quality by reducing the possibilities for interaction without interference. Effective cybersecurity measures also increase the effectiveness of risk regulating mechanisms by influencing the odds of successful betting on trusting behaviour and action decisions (Sztompka, 1999).

It is known that data breaches, as breaches of confidence, can manifest potentially severe security implications and may result in loss of trust in both the trust producing mechanisms and between participants (Kahn and Malluhi, 2010). Therefore, the layering of information security controls required in the transmission and propagation of trust information requires that a model of the domain is produced with which to test the implications that have been made in this critical review of the literature. The conceptualisation of the field of enquiry is included in the next chapter.

3. Conceptualisation and Hypotheses Development

Having critically analysed the literature covering prior research in the problem domain (**Chapter 2**), this chapter moves forward to describe the development of the research model and extends the conceptual approaches found in the extant literature. Most significantly, it outlines the rationale for the classification of information security as a control endeavour that overlaps with the realm of trust in digital environments. The conceptual model is anchored in, and synthesises, previous scholarly work from the long established study of trust formation with the nascent field of cybersecurity research.

3.1 Introduction

That there is a correlation between cybersecurity and trust is recognised in previously published work, and this link has been described both anecdotally and empirically (de Oliveira Albuquerque et al., 2016; Kesan and Hayes, 2014; Nurse et al., 2011). This research extends these observations to investigate the nature of the correlation between security and trust formation online and proposes conceptual and logical research models that seek to explain how and why the twin concerns of trust and cybersecurity are related. The translation of the logical research model into hypotheses is also included alongside a rationale for the choice of the relationships explored.

The following section delineates the requirements that were taken into consideration and the scope of the modelling exercise.

3.2 Research Model Development

A conceptual model of information security and trust in digital environments must be able to communicate the concepts and processes that the logical model is required to possess, prior to forming the research hypotheses based on the logical connections between model components.

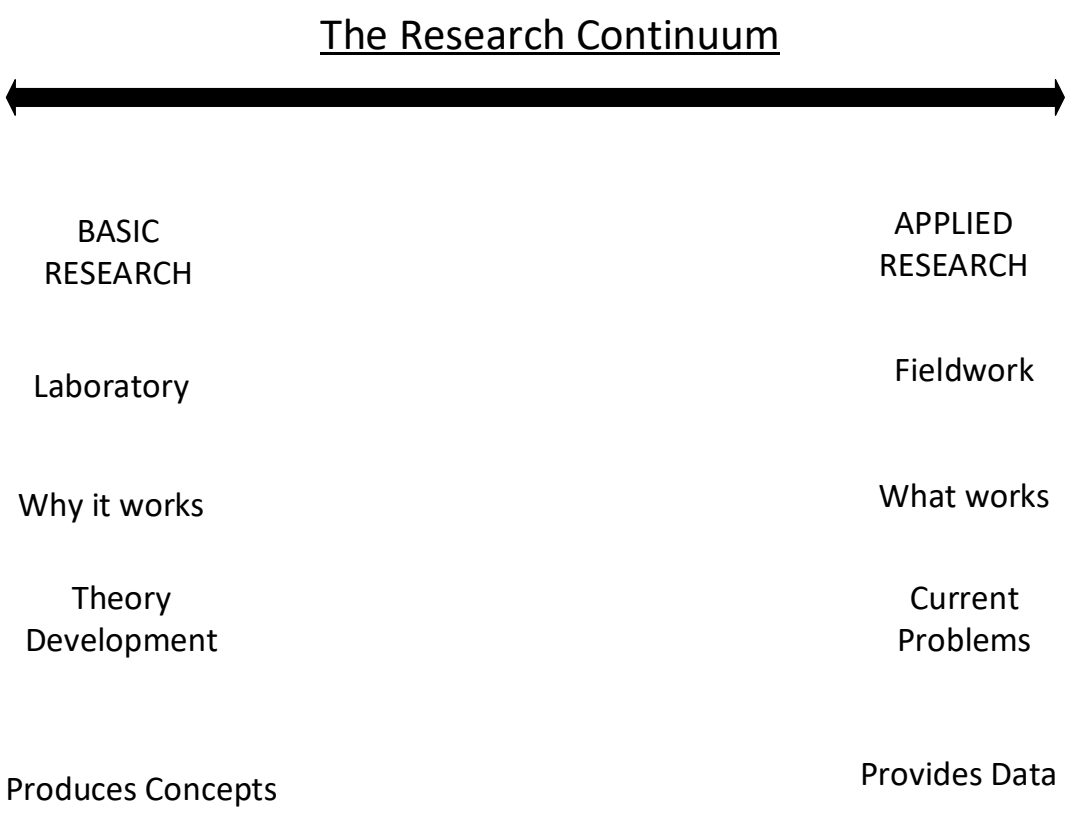
The formation of the trustee-trustor bond is dependent upon the flow of communication between parties (Anderson and Narus, 1990), but the lack of security of the medium in electronic environments is one of the primary causes of the insecurity felt by customers (Phillips, 2002). Alongside the wariness of using a potentially compromised medium to communicate customers must have confidence in the trustee that their relationship information is not broadcast, and that any vulnerabilities that are divulged during trust relationships are adequately protected from disclosure.

It is, therefore, necessary to delineate and separate both the concepts and concerns related to trust from those related to cybersecurity to produce a model that explains the effects of the latent influence of trust and the associated phenomena of cybersecurity concerns. The conjunction of the concepts underpin the major theoretical contribution to knowledge of this dissertation, and the observations,

analysis and implications of this blending of trust and security shape the stance taken by the thesis.

Research outputs form part of a continuum along which the contributions to knowledge are positioned (Figure 3-1). The focus of the research effort was in developing new concepts to guide future work and applications in the information security field and the management discipline. In this respect the current research lies toward the basic research part of the continuum.

Figure 3-1 The Research Continuum



3.2.1 Conceptual Model Development

The first building block to associating the trust and cybersecurity fields of enquiry is based on a taxonomy and interpretation of information flowing between the parties in trust formation. This taxonomy is used to delineate the positive contributions of trust at each level of analysis (interpersonal, person-organisation, organisational and institutional). The second conceptual output and building block is to rationalise the role of cybersecurity in the digital trust environment.

The two concepts of trust and security are united in the process flow model of psychological states outlined in the Theory of Planned Behaviour (TPB) by the flow of information. The conceptual model posits that it is the flows of information sharing between parties and the protective barriers to information disclosure that combine to produce the alchemy of trust. Information-fuelled human behaviour is fused with computer inputs, language and signals to provide trust online, and management assurances and enforcement of cybersecurity policy help to regulate and shape trust as an emergent property of the relationship between the parties from these base elements.

3.2.2 Conceptualising Trust

The psychological motivation for trust from thought to action has been proposed as being formed through a process of belief modelling, intention signalling and considered behaviour, resulting in the formation of trust as a ‘controlled behaviour variable’ (Ajzen, 1985) dependent upon the assessment of past actions, present value

congruence and future focused contingent actions. This conceptualisation of motivation forms the basis of many trust formation frameworks (Mayer et al., 1995; McKnight and Chervany, 2000; McKnight et al., 2002). In evaluating the relative merits of whether to trust in a relationship, individuals take account of innate trusting attitude and their subjective assessment of trustworthiness, as communicated through the reputation of the provider of the online service.

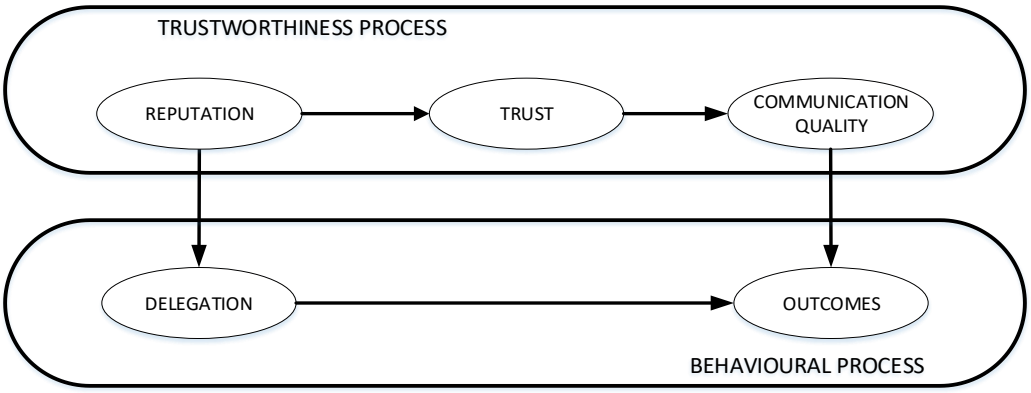
Balancing the two factors of attitude and subjective norms forms a perception of the amount of control in the situation at hand, producing the intention to trust in the relationship and delegate tasks. Where the level of perceived behavioural control is higher individuals may choose to delegate behavioural tasks without the necessity for trust. Task delegation in electronic environments is often a non-option, especially where specialist tasks are needed, for example, payment or processing that can only be carried out by the trusted organisation. Delegated behaviour is a way of operationalising the execution of tasks, and involves the delegated agents acting on behalf of the customer. Delegation online can happen with or without the explicit consent or trust of the user, but as delegated tasks are carried out in the name of the customer then identity preserving security countermeasures are necessary to avoid inappropriate processing or disclosure of sensitive information.

Trust forming online requires the presence of institutional trust measures of the judgement and justice of who to trust because *"Trust is not a matter of blind deference, but of placing or withholding trust with good judgement. We need social and political institutions to judge where to place our trust"* (O'Neill, 2002: vii). Organisations that are allied to institutions assure their customers that they are fitting

candidates for trust by securing and protecting the relationships that sustain their operations (Chen and Rea, 2004). In the digital sphere this is demonstrated by organisations through the judicious exercise of privacy and confidentiality in their dealings with institutions, customers and third party service providers.

The interaction between reputation, trust and communication quality in the delivery of task delegation is shown in Figure 3-2. The positive assessment of reputation engenders the trusting intentions of consumers, which produces an enhanced two-way communication between parties. From the exogenous representations of reputation given by the organisation all actors will benefit from being able to delegate behaviour, but trusting actors can also rely on the enhanced communication qualities afforded by trust towards task delegation and enhanced outcomes. The results of this trust process are developed to provide an understanding of the taxonomy of trust manifestations, discussed in the next sub section.

Figure 3-2 Conceptualisation of Trust



3.2.3 Trust in Practice

The indicators and the socially interpreted presence of trust are discernible in both the online and the offline world. Table 3.1 details the explicit reminders of the existence of the trust constructs by the artefacts of trust found in the conduct of business between humans and organisations in the physical and electronic worlds.

The phenomena of trust in practice shows the inferential presence of institutional trustworthiness, reputation, trust and delegation in real world everyday relationships across three different contexts encountered in everyday life. These contexts represent the research contexts of information security detailed in section 1.1.4 of this thesis as being areas of concern, and which are detailed more fully in section 3.2.9. Each of the levels of analysis is mapped to the relevant theoretical variable from the Theory of Planned Behaviour (TPB) as analysed in section 2.14. Production of the taxonomy allows the ontological phenomena of trust formation to be mapped to the research model variables.

Table 3.1 A Taxonomy of Trust

Level of Analysis	**Retail**	**Banking**	**Healthcare**	**TPB variable mapping**
Trustworthiness (Institutional)	Consumer Regulation	Financial Regulation	Medical Ethics and Governance	Environmental Controls
Reputation (Organisational)	Brand	Presence	Hospital	Belief Generation
Trust (Person-Organisation)	Loyalty Offerings	Account Statements	Medical Records	Intention Building
Delegation (Interpersonal)	Purchase	Banking Transaction	Medical Consultation	Transactional and Relational Behaviour

The adherence to institutional ethics are presented externally by organisations by demonstrating their compliance to regulatory oversight. As examples, a bank will adhere to a banking code, and a hospital will assure the competence of physicians. These assumptions of competence and rule keeping are taken 'on trust' by participants in assessing the reputation of the organisations with which they interact.

3.2.4 Conceptualising Cybersecurity

Trusting relationships in online spaces rely on the party trust between participants and the system trust of the communication medium (Tan and Theon, 2000). The trust formation process is disintermediated by the presence of electronic information systems. The phenomenon of cybersecurity has emerged as a field of

study with roots in computer security (von Solms and van Niekerk, 2013), and adoption of the internet means that the vulnerabilities of computer systems are exposed as externally facing service providers, increasing the area of attack to a wider pool of potential attackers. The complexity of such systems mean that they remain significant vectors of risk through which unauthorised users can access poorly guarded systems.

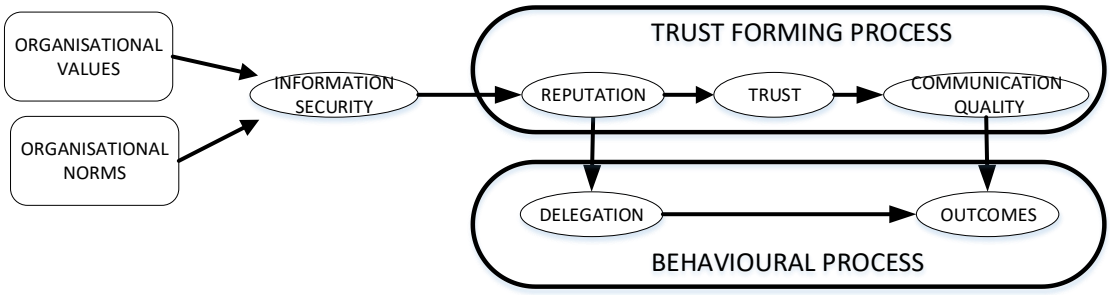
Conducting relationships via electronic means is largely based on cognitive, not affective cues. System trust is based on the attestation of trustworthiness by proxy with the use of 'web seals' and certificates to project trustworthiness credentials. Mathematical proof offered by technologies including Bitcoin and BlockChain offer the customer algorithmic guarantees of trust (Eyal and Sirer, 2014) without the need to trust the organisations that individuals delegate behaviour to. The adoption of cryptography and anonymization for the purposes of online commerce as protection mechanisms ensure that the personal data vulnerabilities displayed by trustors to the trustee are protected in situations where such disclosure in could create risk (ICO [2], 2018).

Generating affective trust in electronic environments removes the dimensions of trustworthiness evaluation that emphasise personal interaction. Online environments are frequently geographically or culturally spread, without these attribute cues. Vendors that may be physically located anywhere in the globe are separated by communication barriers that cannot easily be overcome, but the

communication of trustworthiness is vital to the health of trust evaluation in geographically distant but electronically co-located situations.

Information security is conceptualised as being a formed variable with externally surfaced components of Information Security assurance that act to influence the exogenous cognitive component of reputation. Reputation is the variable that signals trustworthiness and adherence to norms as part of the trust formation process (Figure 3-3).

Figure 3-3 Conceptualisation of Cybersecurity



Cybersecurity then, is concerned with the protection of the flow of information between parties. This communication is made, and has the potential to be intercepted in the formation of trust. Information security requires protection on the 'inbound' journey from belief to behaviour. The data must also be protected on the 'outbound' journey from trusted interactions to customer insights when further processed by organisations. Hence, the protection of personal data must not only be afforded to the provision of protection of sensitive user information, but must be extended to the propagation of privacy-preserving analytic outputs. The taxonomy this umbrella of security provides in the real world is described in the next section.

3.2.5 Cybersecurity in Practice

Cybersecurity is conceptualised as a formed construct consisting of organisational values and norms. These organisational management practices are implemented at each level of analysis. The structure of security protections delineates the protective mechanisms of trust constructs shown in Table 3.2.

Table 3.2 A Taxonomy of Cybersecurity

Level of Analysis	**Retail**	**Banking**	**Health**	**TPB variable control**
Institutional	Critical Infrastructure Protocols			Environmental Trustworthiness Protection
Security	Organisation and sector specific security protocols, Corporate Governance, Ethics, measures and policies.			Protecting Belief and Reputation
Privacy (Confidentiality)	Contextual Product Suggestions	Secure Account Portals	Pseudonymised Medical Records	Trust Intention Protection
Protection (Encryption & Anonymisation)	Purchase Protections	Transaction Encryption	Medical Secrecy	Customer Transaction and Relationship Protection

3.2.6 A Synthesis of Cybersecurity and Trust

For the purpose of this work, the definition of trust, based on a meta-analysis of published trust definitions, is that *"Trust is the confident expectation that a trusting party will engage with other(s) to effect a net positive outcome in situations where risk*

or uncertainty are present without the ability to monitor or control the other party." (**Section 2.3.2**). Combining this definition with that of cybersecurity management as (**Section 2.23),** *"The management of information systems to ensure that the confident expectations of trust are met in online environments by the appropriate controls on transaction integrity, authentication, confidentiality, and non-repudiation."* It is clear from the evidence of data breaches that the online environment presents risk and uncertainty to organisations and individuals (Sen and Borle, 2015). The role, therefore, of the cybersecurity management discipline is to implement suitable controls on behalf of the trustor so that he/ she does not have to perform these monitoring tasks personally.

Cybersecurity provides protective control variables (Table 3.3) that can be utilised to overcome the vulnerabilities inherent in trusting action, by shielding the individuals from the effects of compromise in the willingness to be vulnerable; the vulnerability that is exposed in transactions; the preservation of the confident expectation of trust; and the ability to restrict the opportunistic actions of the trustee. The primary aim of the trust-seeking organisation is to manage the security aspects of cyberspace to generate confidence in trustors by projecting a positive reputation for security.

Security acts as boundary protection to trustworthiness by outlining the permitted and tolerated values and behaviours of organisations. Information confidentiality protects the relationship that is the instantiation of trust as a system of regulative and constitutive rules. Sensitive data protection measures employed by organisations act as assurances to trustors that their vulnerability will not be exposed if they choose to trust.

Cybersecurity measures, therefore, have both causal effects and consequential determinants on the propensity to trust. At the coarsest level of analysis information security is posited to be a causal moderator of reputation and information confidentiality is a determinant of the resulting communication quality. Transaction level protection measures afforded by encryption and anonymisation that ensure the secrecy of task delegation are not part of the research enquiry scope.

Table 3.3 A synthesis of protective cybersecurity and trust

Cybersecurity Element	**Protective of trust element**	**Security Measures**	**Purpose of Informational Measures**
Institutional Security	Institutional Trustworthiness	Legal and Constitutional Protection	Security protects citizens by instructing where trust should be placed.
Organisational Security	Reputation	Reputation and Authority Protection	Security protects the vulnerable customer by providing guarantees of safety and freedom from opportunism.
Information Confidentiality	Trust	Privacy control and Pseudonymisation Protection	Confidentiality preserves the privileged relationship information from improper processing, and enables positive expectations, successful outcomes and relationship growth.
Protection	Delegation	Protection of sensitive data by Encryption or Anonymisation.	Protection defends the vulnerability that the trustor is disclosing to benefit from the trusting action.

Consequent feedback from delegated action by the trustee or their agents amplify or attenuate the perception of the outcomes to trustors. In all instances information flow (feed forward) and evaluation (feedback) are the joining keys or bridge between the security and trust where a priori and posterior belief either erode or sustain the trusting belief based on the information flow towards and as a result of task delegation and actions.

3.2.7 Conceptual Model

The conceptualisation of trustworthiness is based on the influential work of Mayer et al. (1995), and the assertion that trust is based on an assessment of the trustworthy credentials of the trustee (Ability, Integrity and Benevolence). This work was synthesized with the contribution of Ajzen (1985) with the theoretical contribution of the Theory of Planned Behaviour (TPB). This provided the process 'backbone' of the model whereby trustors go through a process of belief modelling, intention signalling and trusting behaviour.

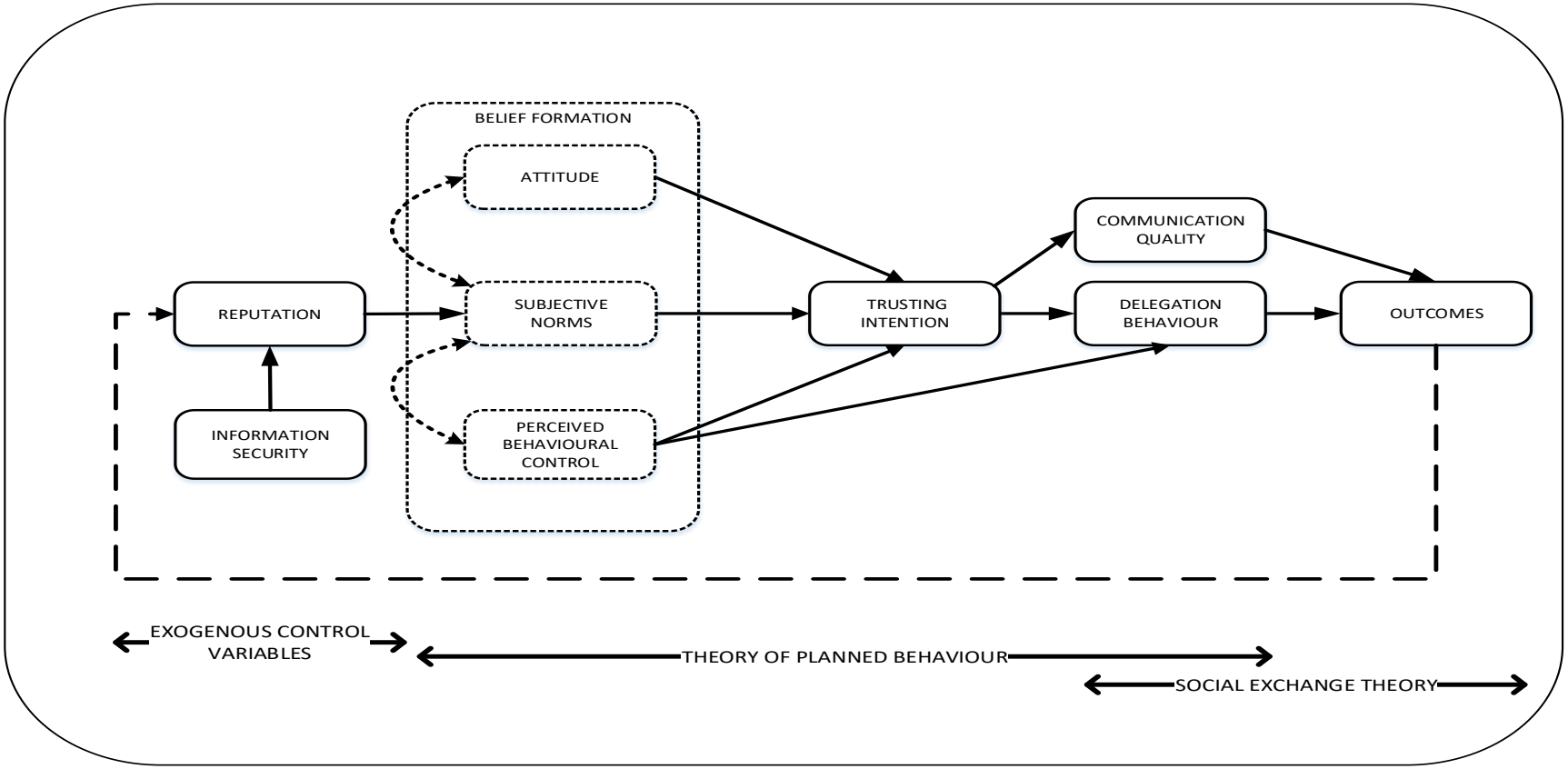
Belief forming (Attitude, Subjective Norms and Perceived Behavioural control) decision selection variables are psychologically weighted to ascertain whether trust is applicable in the situation at hand. If the individual decides that the need to trust is not necessary as there is no information asymmetry present or controls are in place requiring no need to trust they will delegate without trust. Where an asymmetry is present the trustor will have to depend on trusted delegation of behavioural tasks to others but in return receives the relational benefits of increased communication

quality. The intention to trust is enacted, dependent upon the assessment of beliefs formed through the lenses of the past actions, present value congruence and future focused contingent actions. This belief-intention-decision process, in turn, draws on the work carried out by Siegriest et al., (2000) on the Salient Value Similarity of trusted partnership formation.

Behaviour enacted within trusted or untrusted contexts produces outputs, and in the online realm these are the deliverables, records, services or transactions produced by the computing machines and infrastructure. These outputs are accompanied according to the nature of the relationship and the power of the connected parties with outcomes, due to the processes of reciprocity (either direct or delayed) and draws on the Social Exchange Theory (Blau, 1964).

The conceptual model developed as a result of the reasoning process is shown in Figure 3-4. The model shows a progression of concepts from the information security controls acting on the reputation of the organisation as the exogenous inputs to the system. These variables are linked to the TPB belief formation variables, from which the behavioural step of delegation is undertaken with or without the intermediate intention of trust. Where trust is present, the communication quality afforded by Social exchange theory modifies the outputs into outcomes, which in turn produce a feedback mechanism that enhances or erodes the reputation of the trustee.

Figure 3-4 Conceptual Research Model



3.2.8 Logical Research Model

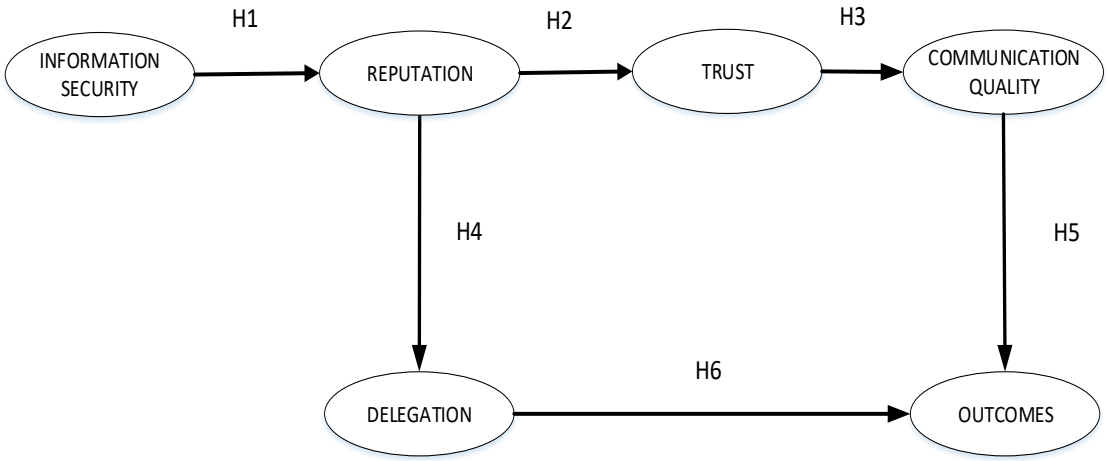
The research model design was logically derived from the concepts contained in the conceptual model (Figure 3-4). The concepts were derived from trust theory research by decomposing the psychological processes operating in trusting behaviour. The psychological decision variables of Attitude, Subjective Norms, and Perceived Behavioural Control are assessed internally by individuals based on the reputational inputs signalled by the trustee party. The output of this internal processing is manifested as delegation. Optionally, individuals may also manifest the intention to trust, which is displayed through enhanced two way communication quality. As Attitude, Subjective Norms, and Perceived Behavioural Control are considered to be variables that are individually assessed, the logical research model provided identical input for each respondent, and the output variables of trust and delegation were used to infer the relative strengths of the internal variables.

The trust constructs are posited to be moderated by the presence of psychological cyber security cues from the supporting information systems where inter-party interaction is mediated by the electronic medium of communication. The independent variable of information security is proposed as an influencer on the dependent trust variables through its incorporation into the reputation of the provider. The constructs in the research model represent the logical inference of the conceptual model by incorporating Information Security and Reputation as exogenous variables that exert a causal effect on levels of the Trust and Delegation constructs. In turn, the presence of Trust produces enhanced Communication Quality that produces Outcomes. This

model extends the prior work carried out by scholars in the field of trust by the production of a conceptually underpinned integrative structural model of trust formation and protection relationships in both social and electronic domains (Figure 3-5).

The transition from conceptual to logical is predicated on the presence of information security as an independent variable which is communicated to potential trustors via the reputation of the organisation. The provision of information about the way information is handled is combined with the available reputation information to provide a perception of the control that a trustor has on the behaviour of the organisation. In line with the TPB, parties can delegate tasks to the trustee based on the subjective norms of reputation, either in a trusted or untrusted fashion. That is, the presence of Information Security and Reputation can be used to infer the safety of both task delegation and Trust. If the party does not trust the organisation, then only the delegation pathway is taken, leading to tasks being undertaken and the outputs from task execution are reported back. If, however, the trusted path is followed, not only is the task executed, but the feed forward and feedback mechanisms of communication are enhanced, resulting in outcomes in addition to the sparse transactional records of task delegation.

Figure 3-5 Research Model of Cybersecurity and Trust



3.2.9 Trust in Context

As researchers it is only possible to understand what is going on in the social world if we understand the social structures that give rise to the phenomena we are trying to understand (Bhaskar, 2014). The inclusion of contextual scenarios gauged the responses to trust in the three common scenarios to evaluate the influence of differing social structures on the information asymmetry in the trust process. The smaller the asymmetry the smaller is the need to trust and where a greater asymmetry is present then the trustor will have to depend on delegation of behavioural tasks to others (Cvetkovich et al., 2002).

Asymmetry of information is not, however, the only determinant of the necessity for trust in dealing with other parties. The inverted-U theory of trust (Gefen and Pavlou, 2006) states that low trust marketplaces are regulated by guarantees that reduce the need for trust. Highly regulated marketplaces manage the rules of conduct

of transactions to reduce the role of social trust as the regulatory instruments of society regulate transactions. This reduces the role of trust to only those kinds of interactions between these two poles, where it is trust that determines the behavioural intentions of individuals.

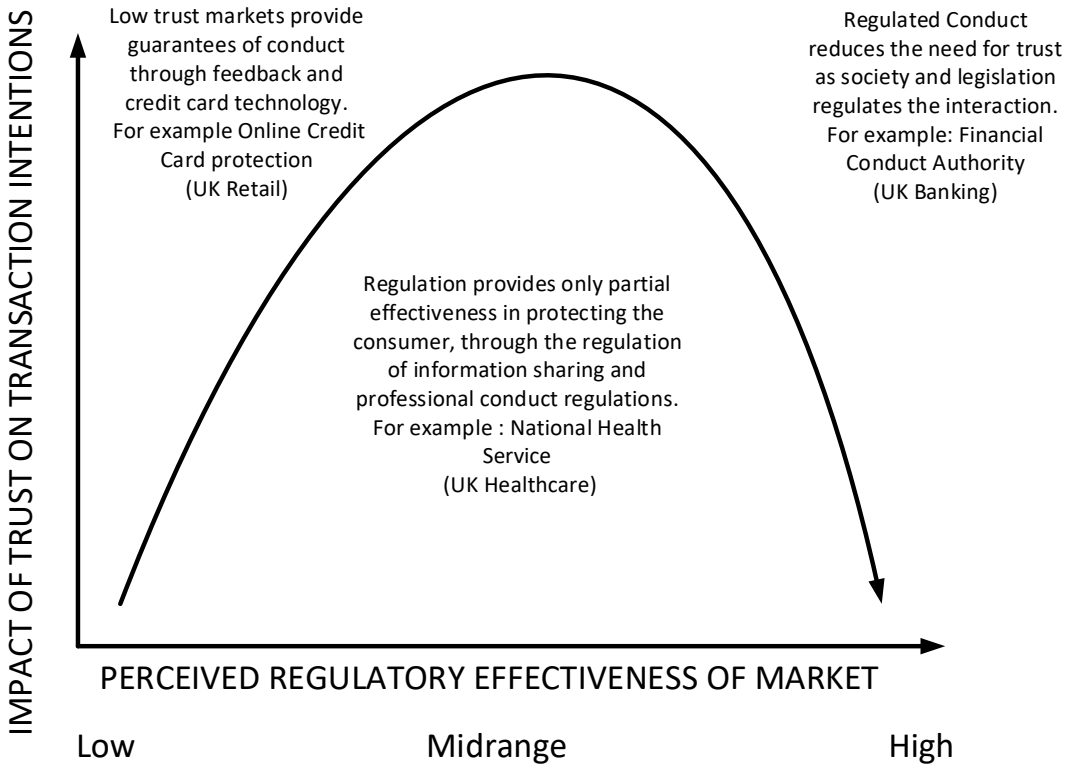


Figure 3-6 Inverted-U relationship between Trust and Transaction Intentions

The presence of context therefore represents a moderating variable that is expected to exert greater influence in some environments than in others. To collect evidence of the behaviour of the research model under differing environmental conditions, three scenarios were chosen to represent major service areas in which the

presence of trust in intentions is effectively differentiated and where information security concerns were present at the time of the data collection. The contexts represent areas of online experience where assessments of performance are often intangible, and the credence attributes of the service are not easy to evaluate.

The scenarios chosen, and the rationale for these choices are:

- **Retail Scenario.** According to the 2019 BRC Retail Crime Survey retailers are spending £162 million and 80% of the retailers surveyed have seen an increase in the number of attacks over the previous 12 months, with phishing attacks and data theft identified as the major issues (BRC, 2019). The burden of information attacks has also fallen on consumers, with the September 2018 information breach at British Airways affecting 380,000 transactions and compromising the personal information details of customers (BBC, 2018)
- **Banking Scenario.** The banking system is an area where cyber threats are constant and adapting (Swift, 2016). Fraud losses to the financial services industry in 2016 amounted to £768.8 million, with 80% attributable to payment cards, and 18% to remote banking (FFAUK, 2017). In addition to the risk of card and financial loss, instances of exposure of personal banking details also occur. As an example, a system upgrade TSB bank in April 2018 allowing customers details to be viewed by others was widely reported (BBC [1], 2019).
- **Healthcare Scenario.** In the May 2017 WannaCry cyber information encryption attack more than one-third of NHS trusts in England were impacted, plus a further 603 primary care and other NHS organisations, including 595 GP practices. NHS

England estimated that more than 19,000 patient appointments were cancelled as a result of the attack. (NAO, 2019)

The examples given are publicly reported manifestations of security breaches involving personal data in three areas of digital interaction that are widely used by members of the UK population. In terms of investigating the effect of digital environments on trust formation there are many other scenarios that could have been chosen, including the use of the internet in public service, supply chain relationships, and law enforcement. The contexts chosen reflect not only a large section of the population where cyber concerns are present, but also represent areas of expertise held by the researcher, allowing insights from experience in these areas to be utilised in the usage scenarios presented to respondents.

3.2.10 Theory Development

The conceptualisation of trust formation in blended socio-digital environments (Figure 3-4) accounts for the fears and realisations of customers who do not know who to trust by proposing that an independent, exogenous variable of information security acts on the trust formation process. Theory development and the contribution to knowledge require that a framework fulfils the key theoretical building blocks, has a legitimate value added contribution, and meets the criteria for being judged as being a contribution (Whetten, 1989).

The roots of psychological influences of cybersecurity on trust lie partly in the work of Maslow (Maslow, 1943) in addressing the deficiency needs of security and

privacy and their effect on the corresponding psychological needs of safety and belongingness. This is motivated by the need to establish trust relationships based on care and protection of the other party (Section 2.17.1, Behavioural motivation). As online interactions have grown, trust in institutions and government has fluctuated (Van der Walle et al., 2008; Chanley et al., 2000) leading to an institutional reliability trust gap that has meant that agents fear the Hobbesian *"force and fraud"* (Hobbes, 2006) over the benefits of trusting online. All transactions are embedded in social relations (Granovetter, 1985), so interactions, whether purely economic or relational are in reality aggregated atomic social transactions. In online environments the social signalling associated with trustworthiness, the interpersonal confidence associated with trust and the visible protections afforded in real world vulnerability protection are lacking. Online social network environments have led to a thinning of thick interpersonal trust bonds (Granovetter, 1973), and an increase of thinner network trust and recommendation mechanisms. This leads to a situation where in dense networks it is safer to trust, but in sparse networks it is advantageous to trust (Kreps, 1996). The nature of the online environment is the 'What' of theory development and includes the variables, constructs and concepts that should be part of the contribution. The formation of the trustee-trustor bond has always been dependent upon the flow of communication between parties (Anderson and Narus, 1990) as a way of signalling the reputation of the trustee in providing trustworthiness and as a way of the trustor communicating needs or expectations. Security provides the components to encourage and facilitate the flow of information sharing. Therefore,

security controls are conceptualised as being boundary protections of the risk taking relationship that provide assurances to trustors that their relationship is well placed.

The underlying 'How' of the development of theory explains the mechanisms by which the contribution explains the relationships between the elements. Following the conceptual model (Figure 3-4), information security enhances the perceived control of the situation by using expressions of shared values to protect customer information, thereby showing the integrity of a partner and increasing the individuals' confidence in their ability to perform a behaviour (Bandura et al., 1980). This extends to identity and personal information protections implicit in the intention to trust that are protected by the trustee ability, and delegating behaviour is protected by the trustee placing constraints on information flow to third parties to show benevolence. The 'How' contribution is that these information security controls produce effects that enhance the effects of reputation in the service of the customer. This viewpoint builds on the existing models of organisational trust theories by positing that security applies the principles of trustworthy reputation throughout the trust formation process (Figure 3-5) to delineate the patterns found in the data, and this led to the research enquiry into how the factors are related by the formulation and testing of hypotheses.

A consideration of 'Why' these information security and reputation factors are important helps to make the assumptions in the theory explicit. It is also necessary to make the definition between customers, who exchange services for payment, and consumers, who utilise a service leaving it to the organisation to create and capture the value created as a result of the interaction (Berthon et al., 2007). As the providers

of services that customers require, organisations can extract a compliance from them for providing the resources (Blau, 1964: 127). The party who holds the resources holds the power, and it is in their interests to maintain the asymmetry of services information with customers, for example, in supplying retail goods. However, in other circumstances providers consider their collected data and services to be the principal in the relationship and the consumers as agents or content providers, for example, in healthcare research. Implementing reputation controls (Section 2.27.1), trustor controls (Section 2.27.2) and relationship controls (Section 2.27.3) help to demonstrate that the organisation has motivation and commitment to treating the customer or the consumer as the principal in the relationship and lessens the need for individuals to be guarded in their monitoring of trustee behaviour. Trustors providing financial and personal details and vulnerability to remote agents could be exposed to the twin risks of adverse selection and moral hazard (Prescott and Townsend, 1984; Klein et al., 2016). These risk conditions arise either through the direct interaction, or via the interaction trustees have with other third parties, including unwanted intruders. Trustors as principals generally suffer from both an information asymmetry, and in the case of cybersecurity this is compounded by a knowledge asymmetry due to the complex nature of the threats and the root causes behind them. They are not only vulnerable to the problems of opportunism presented by poor vendor choice or misrepresentation, but also vulnerable to ongoing moral hazard that may be caused due to incorrectly stored, leaked or shared data. These controls help to modify the beliefs, intention and behaviour of trustors towards trust, and in so doing, increase

the relational benefits and outcomes to gain mastery over events online by information exchange (Tomkins, 2001) as a result.

Schneier (2012:123) characterised the necessity for cyber security as stemming from a need to scale up and fill in the gaps of the normative forces that prevent defection, acting at institutional, reputational and moral levels of analysis. Although norm enforcement and compliance checks are necessary for the effective functioning of structures it does not explain the growth of cyber insecurity in individuals (Hansen, Saridakis and Benson, 2018). The imposition of compliance on agents does not generate psychological security in individuals, and the additional surveillance required to ensure norm adherence may have the opposite effect (Davies, 2016). Although data breaches and security concerns happen to organisations and institutions they also affect the psychological wellbeing of individual agents. Measures that are protective of the structure as well as the agent help to build the trust levels required for relational exchange.

When faced with delegating action without controls individuals may prefer the offline security of true identity or withdraw from trusting any organisations online, foregoing the benefits of social exchange. Alternatively, they can seek an economic return on their data, withholding it until a price is reached at which organisations are willing to trade or it is required for relational purposes. Being the holders of desired information, they utilise social exchange with the protective controls that best protect themselves from the threats that accompany trusting action. Trustors use perceived control as an internal decision information system (Ajzen, 1985) to insulate

themselves from, and to monitor the behaviour of online agents to mitigate where possible the risks of disclosure.

The provision of services by a select few individuals that are not easily obtainable elsewhere create status and power differences, and it is these power differences that make organisations possible. When power in organisations is exercised correctly this leads to a legitimisation of the power in a stable organisation (Blau, 1964). Trust relationships generated through social exchange are generally seen as a social good (Molm et al., 2000; Cropanzano, 2005), providing integrative benefits that are wider than the immediate contract needs of trusting parties through reciprocation and relationships benefits. However, where power is unfairly exercised opposition can develop, and the socialised compliance of agents can lead to an asymmetric relationship in which compliance in an integrative structure is demanded, yet the benefits do not flow to the agents that sustain it (Kong et al., 2014). Security controls act as a necessary brake on the power of organisations to act opportunistically, and use regulatory normative controls to ensure expectations are met.

Having analysed the 'What, How, and Why' of theory development, the limitations on the applicability of the theory were analysed with an assessment of the 'Who, Where and When', the temporal and contextual constraints on generalisability. The mechanisms by which these constraints were explored was through the use of contexts as detailed in Section 3.2.9. Statistical techniques were also applied to the mediation and moderation of variables to explore where and when the theory applied. These methods are detailed in Section 6.8, Mediation and Moderation.

This thesis makes a theoretical contributions in two areas. It extends the Theory of Planned Behaviour to the understanding of how information security affects the intention to trust online by contributing to the understanding of the mechanism by which the stated security values of the organisation correspond to those of the individual through moderation of the perceived behavioural control variable.

This work also extends the understanding of Social Exchange Theory by explaining the role of trust in delegating tasks to organisations through trusted or untrusted delegation and behaviour, differentiating the two behaviours predicted from perceived control by the TPB. Untrusted delegation is seen in the classical view of Social Exchange Theory as being the price of a resource held by an organisation. This research extends this transactional view of interaction by predicting that the enhanced communication quality of trust produces reciprocal outcomes of value to the consumer over and above the output of the transaction. The rise of digital technology in human interactions requires an explanation not found in Social Exchange Theory of the mechanisms by which longitudinal data sharing assurances help to contribute additional value to the security of individuals.

The research investigation aims to demonstrate that information security combined with the traditional attributes of ability, integrity and benevolence advanced by Mayer et al. (1995) provides the values-based motivation that enhances the credibility of organisational trustworthiness in online scenarios.

3.2.11 Research Model Development Summary

This section outlined the development of the conceptual underpinning and rationale for the proposed logical research model and explored how these requirements were met through existing contributions in organisational trust, social exchange and planned behaviour theory. Existing conceptualisations were re-evaluated and critically analysed prior to synthesis as part of the processes involved in the production of the research model.

Conceptualisation and taxonomy production allowed the separate concerns and roles of information security and trust to be blended into a model that encompassed both domains of enquiry. Logical reasoning based on the conceptual model and taxonomies detailed produced the research model of information security and trust formation.

The production of evidence to verify the model is necessary to show the contribution to the development of theory in the area of online trustworthiness and reputation, trust formation using the TPB and Social Exchange Theory. To evidence the contribution of theory development in these areas it was first necessary to deduce research hypotheses based on the logical research model in Figure 3-5, and these hypotheses are formulated in the following sub sections.

3.3 Research Hypotheses

The experimental survey work investigated a number of hypotheses relating to the formation of trusting relationships and their relationships to cybersecurity in socio-technical environments. The hypotheses formed, and the rationale detailing their formation are detailed in the following sub sections.

3.3.1 Information Security and Reputation

The trustworthiness of an exchange partner is based on the perceived information trustworthiness received by an end user, in terms of evaluating the source, the information received and the end user characteristics (Nurse et al., 2011). In TPB terms these variables represent the belief evaluation elements of subjective norms (the trustworthiness of the source), perceived behavioural control (the information), and attitude (end user attitudes) in assessing trustworthiness (Ajzen, 2005).

Reputation has been defined as being an evaluation of a company over time and is based on communication that provides information about an organisation (Gotsi and Wilson, 2001). If this evaluation of information is taken as an assessment of the attributes of an organisation, and reputation is the result of trustworthy behaviour (Hosmer, 1995) then reputation is potentially vulnerable in cases involving imperfect information (Kreps and Wilson, 1982) about that behaviour. Reputation reinforces the communication of norms to trustors by signalling that it is safe to trust (Lee et al., 2005; Anderson and Narus, 1990), so denoting the trustworthiness of the source.

End user attitudes to the source are embedded in the character of the individual and society, and the pre-play communication received from the trustee sets the situational context in which the reputational communication is received (Ostrom, 1999), as explored in Section 2.15, Attitude .

The information that is communicated to the user is viewed in conjunction with the reputation of the source and the attitude to shape the perception of behavioural control that the user can expect. Information and the associated knowledge mechanisms it triggers (Kay, 2006) makes security a higher value than usability or ease of use (Salisbury et al., 2001). Information in the hands of contextually primed end users from a reputable source primes the individual towards an intention to trusting behaviour (Section 2.24, Belief Generation Systems).

As noted by Malhotra et al., (2004) the publishing and communication of privacy policy and security governance information leads to higher levels of trust online. Research into the role of online recommender systems has also shown (Jøsang et al., 2007) that the effect of multiple positive outcomes can enhance the reputation of trustees (Sections 2.24.1, Reputation Management and 2.25.3, Recommender Systems). These controls ensure that not only is the belief in the trustee strengthened by such information, but that the back-up of feedback ensures the decision is well judged and faith well placed.

This hypothesis seeks to ascertain if the receipt of information security information is reflected in an increased perception of the reputation afforded by the

source organisation. This mechanism is posited to strengthen the bases of belief in the trustee by the following mechanisms or tendencies:

- Inferencing generalisations of trust without direct experience (Falcone and Castelfranchi, 2008) by increasing the perception of norms.
- Providing pre-play communication to individuals to trigger socially received attitudes to trusting.
- Increasing the perceived behavioural control open to trustors.
- Protections in online systems decrease the perception of risk and increase levels of delegation to an online party (Pavlou, 2003).

These tendencies combine to produce a relationship between the effects of information security afforded and the reputation of the provider of the information to produce belief in the trustor, marking a point of difference for the current research.

H1: *There is a positive relationship between the level of perceived information security and the reputation of the trustee.*

3.3.2 Reputation and Trust

Reputation is a mechanism that allows a party to have trusting belief in another regardless of any first-hand knowledge (McKnight, 1998). As such, it plays an important role in facilitating the change from generalised trust into one or more classes of instantiated situational trust (Section 2.4, Trust Categories) in a specific referent. As trust is a situational factor of relationships whereas trustworthiness is a quality displayed by the parties which engenders trust (Blois, 1999), the

trustworthiness assurances implicit in the assessment of reputation are more likely to translate into situational trust for the consumer.

Trust online consists of the two components of party trust and system trust (Section 3.2.4, Conceptualising Cybersecurity). The co-existence of reputation and trust does not only apply in personal situations, and has been extensively researched in the context of multi agent systems and computational methods (Jøsang et al., 2007; Xiong and Liu, 2004). Trustworthiness extends to the information systems that are used in electronic environments as well as to the party that controls the systems.

As trust is therefore dependent upon both aspects of party trustworthiness and system trustworthiness to elicit the psychological intention to trust then reputation online is posited to be strengthened by attesting to both information security measures and organisational values as part of prior communication, and this will produce the relationship to be tested that:

H2: There is a positive relationship between perceived reputation and Trust in the trustee.

3.3.3 Trust and Communication Quality

Communication is considered integral to the interpersonal processes of trust building and repair even in virtual environments (Coppola et al., 2004) and trust in distributed environments is heavily dependent on computer mediated communication technology (Jarvenpaa and Leidner, 1999). It has also been shown that the presence of trust indicated enhanced the purchase intentions of consumers

(Gefen et al., 2003), acting as a feed forward mechanism prior to behaviour, and that feedback mechanisms likewise enhance the reputation of trusted sellers (Pavlou and Dimoka, 2006) in post behaviour situations.

Trust uses communication as a lubricant to smooth the wheels of social capital in situations where information is lacking, incorrect or misinterpreted. This extends to future actions as trusting communication responses have also been shown to be anticipatory rather than reactive in nature (King-Casas et al., 2005). Therefore, latent confident beliefs rooted in trust allow for a proactive negotiation and verification of socially constructed security assurances.

It is posited that trust enhances the transmission of meaning and facilitates the feed forward and feedback communication mechanisms involved in online situations. The information exchange and sharing between parties (quality of communication) is therefore an effect of the levels of trust between parties, and the hypothesis to be tested is stated as:

H3: There is a positive relationship between reported levels of trust and the quality of communication between parties.

3.3.4 Reputation and Delegation

The relationship between reputation and delegation is at the interface between cognitive and behavioural trust. It marks the boundary between the willingness to be vulnerable, in which there is no risk, and being vulnerable and exposed to the risks inherent in action (Mayer et al., 1995).

Reputation is a normative reference point for individuals in the subjective reasoning behind an intention to trust, and there is no action without intention (Devlin, 1995). Although this thesis has focused on actions taken within the context of a trusting relationship, this is not always the case. Action may be non-volitional, but in all cases of delegated action a commitment is made to delegate a task to another agent acting in place of the individual. Therefore, it is necessary to have an expectant confidence that they are competent enough to carry the task out. The achievement of goal directed objectives can be made, regardless of the presence of trust, as long as the reliance or ability of the agent (Baier, 1986) is sufficient to undertake the task.

Allied to this, co-operation and delegation in task completion are the defining characteristics of multi-agent systems, as agents typically lack the knowledge, capabilities, or resources to achieve their objectives alone (Griffiths, 2005). Therefore, when taking the decision to delegate online trustors will generally rely on a transitive trust relationship between the system owner and the agents that are delegated to (Castelfranchi and Falcone, 1998). Reputation is the variable that supplies the required connection to institutional mechanisms of behaviour control. These can be institutional, social, algorithmic, or contract based guarantors of the safety of task delegation (Shapiro, 1987).

It is logical to reason that, as reputation is a measure of the safety of both reliance and trusting that there is a relationship between the measurement of reputation and the measurement of delegation to the agent. The hypothesis allows

further investigation of the non-linear relationship between trusting belief and observed delegated behaviour (Gefen, 2008).

H4: There is a positive relationship between perceived reputation and task delegation.

3.3.5 Communication Quality and Outcomes

The outcomes of collaborative behaviour between parties have been cited as an indicator of reputation and trustworthiness in inter-organisational contexts (Yang, Hu and Zhang, 2007). Trust is thought to promote respectful behaviour in translating positive expectation into behaviour (Savolainen and Fresno, 2013).

The quality of communication between parties is posited to be an indicator of positively interpreting and proactively explaining task outcomes as a way to generate the perception control over events (Baron and Kenny, 1986). Control of a situation involves communicating the information needs of both parties. This produces an information and knowledge sharing alliance (Tomkins, 2001), and in trusting relationships this knowledge sharing is perceived to be part of the enduring relationship. For individuals the alliance allows the achievement of personal goals by accessing social capital and the expertise of the trusted organisation, and it allows the organisation to exert a degree of control over individuals beyond the organisational boundaries.

It can be reasoned that, by the process of information sharing, the planning and co-ordination required to negotiate and achieve the proximal and desired goals and

outcomes are more likely to be achieved when the levels of communication quality between parties is high. Therefore, the hypothesis tested for this is stated as:

H5: There is a positive relationship between the communication quality between the parties and the outcomes of delegation.

3.3.6 Delegation and Outcomes

The proactive action decision model posits that trustors evaluate and act upon the information that is given to them from environmental (contextual) cues; the channel that those cues are received from; warning messages that they receive and the characteristics of both the sender and receiver of the message prior to taking protective action in situations of risk (Lindell and Perry, 2012).

The information received, heeded and comprehended by customers, when adjusted for other cues is a function of the trustworthiness of the source (Nurse et al., 2011), so by protecting themselves from risk by delegation consumers place higher credence on protection assurances from trustworthy partners than they could produce by taking action themselves.

Action produces outputs and environmental change that express the free will of the individual in volitional situations, and show the compliance of the individual with the trustee in situations where action is not optional (Sztompka, 1999). Production of electronic systems delegated output acts as feedback to interpret the meaning of the actions to the individual. Therefore, it is reasonable to say that there is a relationship present that can be expressed in the research hypothesis stated as:

H6: There is a positive relationship between task delegation and the perceived outcomes of delegation.

3.3.7 Research Hypotheses Summary

The research model constructed in the first part of this chapter was used to derive the hypotheses to be tested. A brief rationale for the selection of each was included in this section, and are shown in summary in Table 3.4.

Table 3.4 Research Hypotheses Summary

Hypothesis	**Research Hypothesis Statement**
H1	There is a positive relationship between the level of perceived information security and the reputation of the trustee.
H2	There is a positive relationship between perceived Reputation and Trust in the trustee.
H3	There is a positive relationship between reported levels of trust and the quality of communication between parties.
H4	There is a positive relationship between perceived reputation and task delegation.
H5	There is a positive relationship between the communication quality between the trustee and the trustor and the outcomes of delegation.
H6	There is a positive relationship between task delegation and the perceived outcomes of delegation.

3.4 Conceptualisation Chapter Conclusion

The role of electronic environments can promote or demote the perception of the role of trust in human actions. On the one hand encryption and algorithms promote the safe disclosure of vulnerability information to securely achieve remote tasks, yet on the other hand, the lack of co-location and the use of third parties has led to concerns that security concerns pose risks to consumers that are beyond their control, with consumers taking a 'transaction over trust' approach to online exchanges (Hoffman et al., 1999).

To direct the research enquiry into whether information security has a bearing on trust formation online it was necessary to build a conceptual model of the research domain of interest, rooted in the prior literature. Critical analysis of the manifestations of trust and cybersecurity were grouped and synthesised and a conceptual model of the problem domain was produced. The conceptual model allowed a logical model of relationships to be derived, from which the research hypotheses were isolated. Isolating the component parts of the model allowed each of the rationalised statements to be tested as part of the exploration into information research and trust.

Prior to testing, it was necessary to translate from the research model derived in this chapter into a choice of methodology and strategy with which to test the hypotheses, and this is given in the next chapter, **Chapter 4, Research Methodology**.

4. Research Methodology and Method Choice

4.1 Introduction

In the previous chapter the development of the conceptual and research models were introduced and the associated testable hypotheses were established. The transition from conceptual model to research findings requires a transformation of the model by way of logical reasoning approaches towards the selection and justification of a research methodology with which to test the research hypotheses.

Prior to commencing the research investigation it was necessary to select and construct a rationale for the structure of the research methodology. From this selection the analytic approaches that were taken to test the model, investigate the hypotheses, and interpret the statistical outputs resulting from the research effort was constructed.

This chapter outlines the process by which the research methodology and the methods of investigation were selected. The first section details the characteristics a paradigm needs in order to be selected for the research enquiry. The second part details an appreciation of the structure and assumptions that underlie the dominant research paradigms prior to selection. After selection of the paradigm and associated methodology, the final part of this chapter details the research strategy and methods

employed toward testing the model and hypotheses using observations and data relevant to the problem domain.

4.2 Paradigm Characteristics

The characteristics that stem from a research paradigm choice are ontology, axiology, epistemology and methodology. A definition of each of these cornerstones of research is given along with the variations in emphasis that differentiate research paradigms are given in the following sub sections.

4.2.1 Ontology

The philosophy of ontology deals with the nature of reality. In the consideration of the nature of reality the attribution of meaning to things is achieved by considering the essence of being or becoming. An understanding of the nature of being is important for the researcher so that they are able to assign meaning to the reality that is being observed. Thinking about reality has two viewpoints, those of the essentialists (Platonic idealists) and the nominalist school of thought.

Essentialists take the ontological view that to understand the nature of reality it is important to 'go back to the form', or the ideal of what something is. This ideal is an abstract concept of the thing in question that encapsulates the core aspects of the item in question. Contrary to this view is the opinion of the nominalists who emphasise the grounded manifestations of reality. This takes a 'back to the facts' view

of reality and that the nature of reality can only be known from its' manifestations (Bestor, 1988).

The philosophical perspectives and debates between proponents of essentialism and nominalism reflect the ways in which reality can be known, either from the essential idea to the form (theoretical), or from the nominal form towards the idea (phenomenological) (Bestor, 1988). As such, essentialists will tend towards the generalisations seen in the research, and will take a nomothethic research approach, whereas nominalists will seek specialisations and specificity in form by taking an ideographic viewpoint. Ontology embeds the axiology of the researcher and this is examined in the next sub section.

4.2.2 Axiology

Axiology, or the values that lie behind the beliefs of the research is also an integral consideration of paradigm choice (Guba and Lincoln, 1994). Axiology deals with the ethics and values that the researcher brings to the research, and are considered in the things the research judges to be valuable in the field of enquiry. That the research centres on the relationships between cybersecurity, information and trust and the role and power of organisations to determine the user experience gives an indication that the researchers' interest lies in the role of the organisation in these particular areas of digital life.

The ontological and axiological views of the researcher informed the epistemology of how the researcher knows and can justify the beliefs on which their enquiry is based, and is covered in the next sub section.

4.2.3 Epistemology

The origin of the word epistemology stems from the Greek word for *"know, or know how to do"* (OED, 2019). The philosophy of epistemology deals with the questions of the nature and scope of knowledge, and deals with the theory of how it is possible to rationalise beliefs.

This consideration of 'knowing' how to 'know' knowledge is relevant to the research problem and epistemology seeks to answer the questions that arise around how we know what it is we know about the underlying reality. Epistemology captures the rationale and the knowledge that arises from the chosen paradigm of the researcher. This knowledge occupies a space between the positivist view of reality independent of the observer, or the constructivist view that reality is actually a subjective one, as constructed and experienced by the observer.

The subjectivity of experience arises in social science research because the generative mechanisms arising from the workings of reality must be viewed through a sociological lens. In this way *"different conceptual schemes generate different, and apparently inconsistent descriptions of the same reality"* (Searle, 1995:163). This echoes the imperfect and probabilistic viewpoint of the post positivist paradigm and the epistemological approach that follows. The critical realist research approach

encapsulates the position of the post-positivist philosophers who acknowledge that knowledge is based not on unchallengeable truths, as human knowledge is unavoidably conjectural. The assertion of these conjectures are warranted, or more specifically, justified by a set of warrants (Popper, 2005), and these warrants can be modified or withdrawn in the light of further investigation. Post positivism generally retains the idea of objective truth and the post-positivist critical realist recognizes that all observation is fallible and has error (Fischer, 1998). All theory is revisable and by taking a critical realist stance to the research the ability to know reality with certainty is questioned.

The epistemology of direct realism relates to the experience of the events generated by reality and the sensations that are conveyed. Critical realism, as well as taking into account these sensations also takes into account the mental processing that happens after the sensation is conveyed. Critical realism takes the epistemological position that what we experience are sensations, the images of the things in the real world, not the things directly. By tempering the experience of the real through the lens of mental processing and experience the emergence of the real is not merely causal, but influenced by the social (Smith, 2005).

Directly observable phenomena provide credible data and 'brute' facts (Searle, 1995:27). Whereas a direct realist approach would posit that insufficient data means inaccuracies in sensations the critical realist would argue that the phenomena create sensations that are open to misinterpretation. When applied to epistemology the

critical approach to realism generates a focus on explanation within a context or contexts, as opposed to the multiple convergent empiricist viewpoint of facts.

4.2.4 Methodology

The methodology used to investigate the research hypotheses and the conceptual model of information security and trust in digital environments represents the actualisation of paradigm choice, incorporating the philosophical ontology, axiology and epistemological approaches that are consistent with establishing the veracity of the research hypotheses.

The method of scientific inquiry was followed by formulating the research hypotheses in a form that could conceivably be falsified by tests on observable data. Therefore, a test that runs contrary to predictions of the hypothesis is taken as a falsification of the hypothesis, whereas a test that does not run contrary to the hypothesis corroborates the theory (Popper, 2005). The strength of the hypothesis lies in the explanatory value of competing hypotheses by testing how stringently they are corroborated by their predictions.

4.2.5 Paradigm Characteristics Summary

This consideration of the ontological, epistemological and methodological approaches used to pursue the research indicate the pathways to knowledge that the researcher can follow. The assumptions and techniques of enquiry that these approaches to knowledge have is encapsulated in the research paradigm for enquiry.

The major research paradigms, and their characteristics to the problem of knowledge are detailed in the following sections.

4.3 Research Paradigms

Methodology choice was shaped by the research paradigm, or research exemplar, that guided the completion of the work. Research paradigms bring into the research process *"a loose collection of logically related assumptions, concepts, or propositions that orient thinking and research"* (Bogdan and Biklen, 1998:22), and a research paradigm assists the research process by allowing agreement on how problems should be approached by using a common understanding to clarify the assumptions of the researcher about their view of the nature of science and society in a manner so as to be understood and addressed by other scientists (Kuhn, 2012). Paradigms allow reviewers to understand how other researchers have approached their work, and enables the researcher to plan a route through the investigation by allowing an understanding of where it is possible to go and where they are going (Burrell and Morgan, 2017).

According to Guba (1990), research paradigms can be characterised through their ontology, epistemology and methodology. The elements of a research paradigm choice should address these three elements to give a fuller understanding of the questions of what constitutes reality, how things about reality are known, and how the researcher should go about finding the reality out. A critical consideration of the characteristics of the main research paradigms are made in the next sub sections.

4.3.1 Positivism and Constructivism

Positivism and constructivism are the two of the dominant paradigms of IS research (Smith, 2005) and social science research (Hallebone and Priest, 2008). These paradigms represent the major philosophical poles of enquiry and describe different approaches to researching the nature of reality. These elemental research paradigms frame the fundamental assumptions and beliefs as to how the world is perceived and serves as a thinking framework to guide the behaviour of the researcher (Jonker and Pennink, 2010).

4.3.2 Positivism

Researchers utilising a positivist approach work with observable social reality (Hunt, 1991). They seek to approach the problems of research in a value-free way and conduct research as external actors to the substance of the data collected. The positivist approach to research is typified by the use of scientific method to develop specific theory and hypotheses which are quantitatively measured by researchers using established research procedures (Warfield, 2010).

When applied to social sciences the positivist approach seeks to discover general scientific laws of cause and effect that govern not only the physical world, but also extend the scientific method to the interactions in society (Comte, 1975). This takes the form of observed event regularities, general laws and the prediction of outcomes (Mingers, 2003). Conversely, a constructivist / interpretivist stance to approaching and understanding problems can be taken, and is outlined in the next sub section.

4.3.3 Constructivism

The constructivist paradigm involves the way humans try to make sense of the world. Whereas the positivist stance views research problems from a position of rational verifiable brute facts the constructivist is concerned with the discovery of ways of experiencing action in society through interpersonal or common meaning expressed in language, institutions and practice (Schwandt, 1994). Although it is possible to reason that some participants will appear to act subjectively, the constructivist research stance seeks to utilise the convergence of opinions with which to draw conclusions about the general features of the described reality (Cresswell, 2017).

Both positivism and constructivism are engaged in a search for reality. Research undertaken from a positivist perspective seeks knowledge gaps to investigate, whilst the constructivist research paradigm takes meaning to be a social constructed interpretation of the nature of reality (Mertens, 2005). As each paradigm presents a view of reality that is competing and irreconcilable with the other (Kuhn, 1974) it stands to reason that the comprehension of science can never rely wholly upon "objectivity" alone. It must take into account subjective perspectives as well, since all objective conclusions are ultimately founded upon the subjective viewpoints of researchers and participants.

In attempts to reconcile the duality of positivism and constructivism other paradigms of research have been proposed to reconcile the two worldviews presented

by positivism and constructivism. An overview of these paradigms is covered in the following subsections.

4.3.4 Post-Positivism

Post-positivists believe that a reality exists, like positivists do, though they hold that it can be known only imperfectly and probabilistically (Guba and Lincoln, 1994). The true state of the world can only be assessed subjectively and partially, and the constructs that are being tested are related to the socially constructed notion of trust rather than hard physical fact (Moorman, Zaltman and Deshpande, 1992). The implication of the post-positivist view in social research is that there is no separation of the researcher and the researched, but an acknowledgement that biases can and do exist in the work that must be acknowledged. All research is value-laden (Rudner, 1953) and the researcher is biased by world views, cultural experiences and upbringing. Viewpoints that encompass the post-positive view of reality include the Direct and Critical realism paradigms discussed in the next sub section.

4.3.5 Realism

The generative properties and mechanisms of the real provide the possibilities of the actual and are manifested in empirical observations (Archer et al., 2013). The social construction of the actual contains the structures that are communicated between human beings via the medium of language and implemented through the flux of processes, experiences and practices. Therefore, the starting point for critical realism as a philosophy is ontological, not epistemological (Smith, 2005).

At the core of scientific, or direct realism, is a belief that successful theories are representative of what exists, through the production of concepts and theories. However, in social worlds, the Humean notion of the constant conjunction of events does not exist, so predictions become replaced by tendencies and generalisations (Smith, 2005). Emergent structures (for example, trust and security) are the described tendencies, or social facts, revealed through empirical enquiry and shared through language, thinking and experiment. Reality is constantly regulating experience, and manifests itself in the theory-practice inconsistences that result. Therefore, researchers are forced to think in realist terms for the research to have meaning and promote change in the social world.

The concepts of the usefulness of research in the social world are an inherent part of pragmatism, which is discussed in the following sub section.

4.3.6 Pragmatism

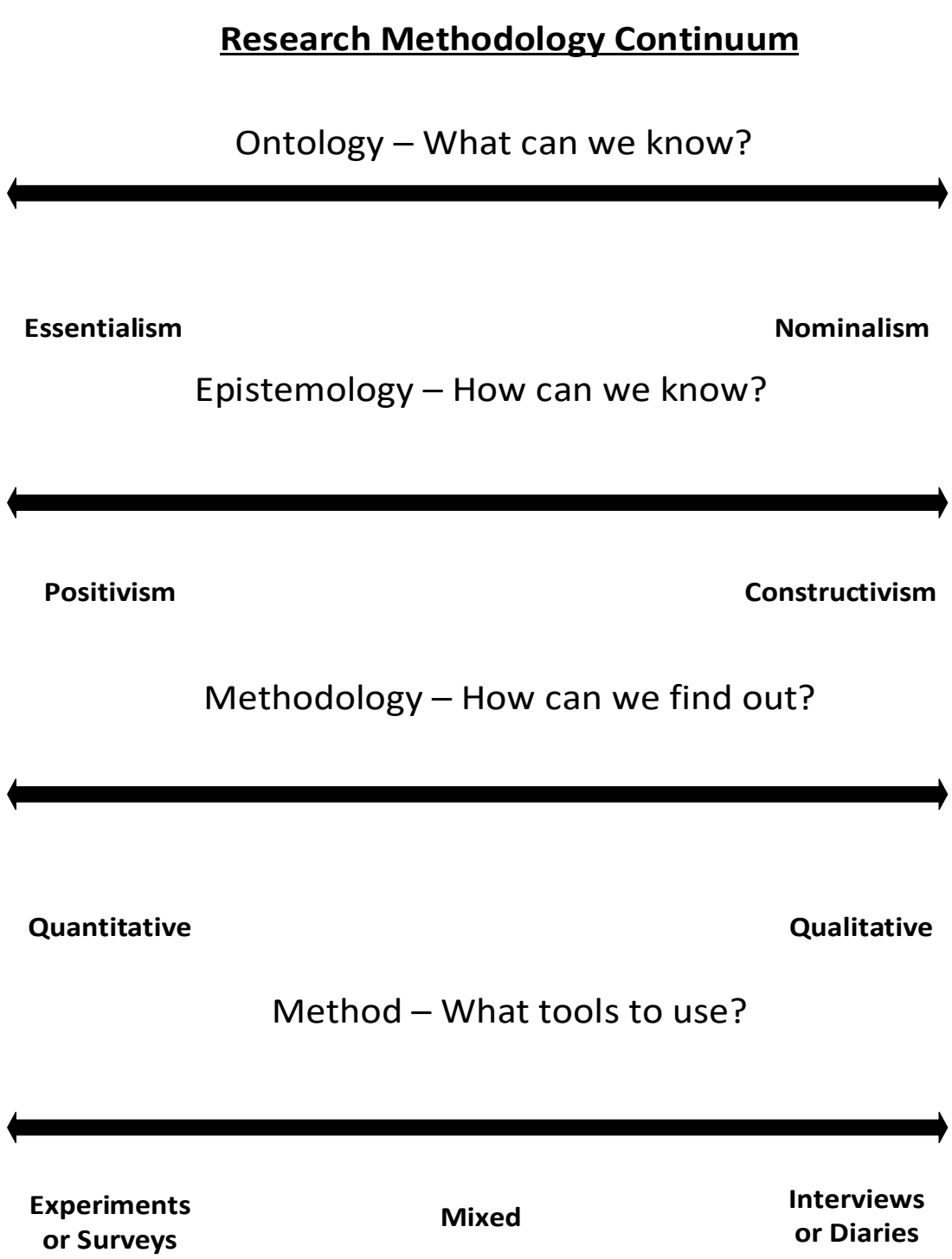
The pragmatic paradigm of research addresses the usefulness of the outcomes. The meaning of concepts is specified purely in terms of the actual practical effects that the concept holds. This promotes a rational consensus theory of truth as that which would come to be believed by a community of scientists in the long term, rather than as correspondence to reality (Habermas, 1984). That if there is no purpose to the work making an impact on everyday behaviour then there is no necessity to do it.

4.3.7 Research Paradigms Summary

Having evaluated the dominant paradigms in the field of enquiry and the characteristics of ontology, axiology, epistemology and methodology they encapsulate. Researching the interfaces between cybersecurity and trust required a paradigm to guide the research effort through a process towards conclusions. It provided a philosophical direction of enquiry through which the complexity, richness and interdependence of the research constructs were simplified. The paradigm choice patterned the interpretation and aided the synthesis into new work.

The next section analyses the methodology choice made given the conjunction of the research aims, model and hypotheses with the choice of paradigm and research approach. The considerations made in the choice of research methodology were considered in terms of the research continuum shown in Figure 4-1 (after Newman et al., 1998:21).

Figure 4-1 The Research Methodology Continuum



4.4 Methodology Choice

The choice and the justification for the methodology employed in the research needed to accommodate both the generalised objectivity of reality as observed by multiple fallible observers alongside how the observed phenomena reflect the world view of those observers.

4.4.1 Introduction

When considered as a taxonomy of academic disciplines management research may be characterised by four key properties (Tranfield and Starkey, 1998:345; Becher, 1989):

- It is characterised by a body of theory that is not universally subscribed to by all members of the field and has no unifying paradigm.
- It is applied in nature.
- It is divergent in terms of shared ideology and values.
- There is a low ratio of people to problems studied and thus research focus and activity is fragmented.

As a result of these characteristics knowledge production in the management discipline emerges incrementally by developing theoretical structures that may not follow any given disciplinary map. Management research is non-reductionist in nature and that researchers should take a *"catholic yet carefully defined approach to the making of quality judgements"* (Tranfield and Starkey, 1998:353). Blending the management discipline needs to be congruent with information systems research, an

area where the extant research is dominated by the positivist and interpretivist stances, but which displays persistent theory-practice inconsistences (Smith, 2005). Neither a positivist nor an interpretivist stance appears to fully address these inconsistencies

4.4.2 Ontological Position

The representation of reality is contained within the described concepts of the models used to test the hypotheses. These constructs were derived from an analysis of the prior literature, and represent an essentialist point of view. The produced effects of the constructs, or nominalist data, which were collected as part of the research enquiry were used to evidence the existence of these factors and mechanisms as part of reality. The ontological approach to this research taken was a nomothetic one, whereby the essential features of the research were deemed to hold more insight into the nature of the problem than the viewpoints and meaning of individual users.

4.4.3 Epistemological Position

The polarising views of reality require that the use of positivist scientific method in social research is tempered by an appreciation of the constructivism that is a feature of social situations. The post-positive, realist and pragmatic paradigms can be employed to manage the oppositions inherent in the positivist and constructivist paradigms and guide the research path to accommodate both schools of thought.

Presupposing the notion of existence of the positivist notion of external reality as *"there are material objects to be met with in space"* (Moore, 2014:15), this external space represents a way that things are that is independent of all representations of how things are. As such, the notion of reality represents a space of possibilities and the research must address how the mechanisms and structures of the real and the events generated there are experienced, either directly or critically. Indirect observations of a presupposed reality requires a socially constructed world and therefore requires the approach of a critical, rather than a direct, realism (Archer et al., 2013). Critical realism has the ability to transcend the dualism presented by positivism and interpretivism by asking *'what are people and societies like that make them possible objects of knowledge?'* (Smith, 2005). The combined study of physical machines and the interaction with human psychology makes the critical realist approach to knowledge a compelling paradigm in the production of knowledge in the socio-technical environment of enquiry.

4.4.4 Methodological Position

Social research values both objectivism and subjectivism in its interpretation. The objective aspects of data collection and data analysis are weighted alongside the way that the survey participants attach their own individual meanings to the model constructs and the way that they think those constructs should be implemented. This emphasises "*the details of the situation to understand the reality, or perhaps a reality working behind them*" (Remenyi et al., 1998:35). Therefore, the research setting of quantitative and qualitative research methods is socially shared, historically produced

and general to a social group. As a result, both qualitative and quantitative research methods are equally valid ways of representing and analysing the social lens through which reality is observed.

4.4.5 Methods Approach

The collection of data is an endeavour that is contained within a background of the context within which it is collected. This is applicable to both primary and secondary sources of data on social interactions, and secondary data must be detached from the original setting to be repurposed for other uses. The contextual, temporal and restless nature of cybersecurity concerns required that new data was required with which to critically analyse the reality of the regulation of trust. As a result the data that were collected to test the research hypotheses was collected from primary sources by way of survey respondents. A fuller account of the research strategy and methods used is detailed in Section 4.5.

4.4.6 Methodology Choice and Justification

If knowledge of reality is a result of social conditioning and cannot be understood independently of the social actors involved in the knowledge derivation process (Dobson, 2002) then the researcher is seeking to observe a knowledge of reality without viewpoint in an immersive social world. If this reality can only be observed through the kaleidoscope of social structure then a critical appraisal of the processes that underlie the observation of reality is necessary to understand the role of the real in the manifestation of the research observations.

The analysis used to originate the hypotheses were based on the essentialist tradition of form, and proved with data on the nominalist phenomena of cybersecurity concerns. The knowledge gained from this approach provided the balanced academic construction of the elements of trust and the human processes involved by providing a synthesis of the underlying latent concepts with phenomena, as opposed to a positivist composition consisting of the assembling or arranging of parts, in discrete stages, into larger structures (Hibberd, 2006). Testing the hypotheses required that the social ideas were translated into objects that would provide an "objective" view of the reality in play. This approach ensured that quantitative statistical techniques and methods were then in scope to provide inferential analysis of the resulting experimental outcomes.

As social systems are inherently open and cannot be closed off from their environment experiments are reliant upon a multitude of factors, all of which may not be known or controlled in the experimental methods used. Controls on the dimensionality and reliability of the attributes of the variables were required to provide triangulation of the viewpoints of reality (Jick, 1979). The truth of theory is an attribute of that theory in a transitive context that corresponds to how accurately it represents the phenomena it refers to in the intransitive reality (Smith, 2005). The dimensionality of the problem space meant that the theoretical contributions of the research drew their authority from explanatory power, rather than on prediction of outcomes.

By signposting the beliefs about ontology and the process of creation of knowledge, the choice of research paradigm was the critical realist approach. The research approach that was followed tends toward the 'sociology of regulation' of social phenomena, status quo, order, consensus, integration and cohesion, satisfaction of needs in dealing with the actualities of trust in dynamic socio-technical systems. In particular, the symbolic interactionism (Blumer, 1986) of actors in a networked computer environment underlines the continual process of interpretation and adaptation that actors undergo in this area.

The merging of people, circumstance and timing involved the critical realist stance being taken by the researcher to better understand the background of the meanings pertinent to the research questions. Justification of the research approach of critical realism was based on the framing considerations of the ontology and epistemology of the problem domain that were translated into the methodology and methods by which evidence was sourced and analysed. The research strategy employed to direct these analyses is detailed in the next section.

4.5 Research Strategy

To balance the need for an consensus view of reality with the encapsulated nature of the social setting in which it is situated, using a critical realist stance to cybersecurity management research involved creating a research strategy of collecting data on phenomena based on objects to minimise the risks of confirmation or researcher bias in the representation of the reality of trusting interactions online.

The strategy and design choices that were followed and the associated methodologies related to the conduct of the research are outlined in the following sub sections.

4.5.1 Conceptual Design Strategy

The conceptual model used in the research (Figure 3-4) was arrived at using an abductive reasoning approach whereby the hypotheses are arrived at by a form of logical inference which starts with an observation then seeks to find the simplest and most likely explanation (Haig, 2008). In abductive reasoning, unlike in deductive reasoning, the premises do not guarantee the conclusion. One can understand abductive reasoning as inference to the best explanation. It allows the inference of the causes of behaviour from the consequents, although observation of these consequents may be due to different causes, including the structure of the construct, the interpretation of the literature review and of the background of the researcher.

4.5.2 Reflective and Formative Modelling

A reflective modelling strategy was employed to discover underlying relationships and determine the strength of the hypotheses produced. Using a formative model of measurement for the research model requires that causality flows from the indicator to the construct. Formative indexes of constructs do not make any assumptions about the interrelationships between indicators and changes in the indicators form changes in the associated construct. In reflective (or effect) measurement models causality is in the opposite direction, and changes in the indicators reflect changes in the latent construct (Edwards and Bagozzi, 2000).

Formative measurement models are dominant in the economics and sociology, reflective measurement is more widely used in psychology and management disciplines (Coltman et al., 2008).

The aim of the research analysis was to ascertain whether the hypotheses were congruent with the observed effects, and consistent with the reasons upon which they were predicated. As the objective truth in this situation cannot be determined beyond doubt, only within probabilistic boundaries due to the psychological nature of the latent constructs, the results can only orient towards the best explanation of the observed behaviour.

The processes of hypothesis testing using exploratory and confirmatory analysis strategies are detailed in the next sub section.

4.5.3 Exploratory and Confirmatory Analysis

The use of exploratory and confirmatory methods in research is related to the extent to which the research is grounded in discovering and exploring new phenomena (Losee, 1997) relative to the prior theorisation and established work in the area of interest.

Exploratory analysis methods are used in cases where the definition of possible relationships in only the most general form is required (Hair et al., 2010). The use of exploratory methods was incorporated into the research methodology in consulting experts during the construction of the model, executing a qualitative card sort methodology to rank construct items and their meaning, and in gathering post

evaluation feedback during the pilot questionnaire phase. Confirmatory analysis involves the use of techniques that allow the method and data define the relationships between the objects of analysis (Hair et al., 2010). Confirmatory methods are used to confirm the presence of pre-specified relationships. The use of confirmatory strategies for analysis were included in the research in the use of Confirmatory Factor Analysis, multivariate and bivariate relationship analysis techniques, and Structural Equation Modelling.

The combination of exploratory and confirmatory factors methods in the research strategy ensured that the relationships between the objects of enquiry were examined in an exploratory fashion to determine firstly that the relationships were possible, followed by the confirmatory analysis to test the hypotheses presented by those relationships.

4.5.4 Full Information and Contexts

Use of the critical realist paradigm implicitly recognises that there is a difference between the reality, and the differing interpretations of that reality. Comparing the stability of the full information model with that of contexts highlights the differences that these asymmetries have on the respondents. The contexts chosen in **Section 3.2.9, Trust in Context** describes areas of active data breach concern that were used as 'vignettes of digital life' in the survey questionnaire tool.

4.5.5 Research Strategy Summary

This section discussed how the choice of the critical realist paradigm of investigation influenced the methodology that was employed in the research strategy. The strategy encompassed the reflective measurement of constructs; how the collected data was handled in both an exploratory and confirmatory manner; and the analysis of the collected data in both a full information and contextual capacity.

The strategy employed for the collection of data as part of the research was carried out in three distinct phases, initial; pilot; and final data collection. Each phase had differing objectives, with the overall aim of data collection being the collection of responses with high validity suitable for analysis. The implementation of the strategy through the data collection process is described in the next sub section.

4.6 Data Collection

The purpose of the data collection phase was to gather primary data with which to test the research hypotheses and model outlined in **Chapter 3**. The processes followed for collection of data were guided by the type of data and analysis being performed. Quantitative data gathering was by means of an initial pilot online questionnaire and a full online survey questionnaire. Details of the timescales for collection, the tools that were used for the capture, storage and analysis of the data collected, and the ethical approvals granted are given in the following sub sections.

4.6.1 Data Collection Tools

The initial exploratory phase of the research enquiry utilised a qualitative card sort data collection method. Content selection, participant selection and card preparation were identified as part of a card sort exercise (Sekhon et al., 2014; Spenser and Warfel, 2004). The initial participants used the preliminary selected item set printed onto standard record index cards. Participant feedback was gathered to improve the flow, syntax, understanding and ordering of the final card sort constructs and item stems.

Conducting a card sort exercise enabled the viewpoints of different observers of the problem domain to classify items to the relevant constructs, even where prior research in the field existed. Each respondent was asked to partition a set of items into different groups on the basis of their 'similarity,' 'relatedness,' or 'co-occurrence'- depending on the particular application (Rosenberg and Kim, 1975). This allowed triangulation of the research constructs, by including multiple indices for each proposed construct (Jick, 1979) and taking into account a synthesised view based on the perspectives of multiple fallible observers. Card sorting offered numerous advantages, including ease of administration, low susceptibility to experimental demand characteristics, economy in handling large numbers of objects or stimuli, grounding in a theoretical framework, and utility with different types of objects (Whaley and Longoria, 2009). Details of the card sort exercise are given in Section 5.2.5.

The pilot and final data were collected and administered by use of online survey tools. Online surveys have advantages in scale, lower cost, availability around the clock, ease of distribution and participant anonymity, but statistically neither enhance nor diminish the consistency of responses or the integrity of the test questions (Riva, Terruzi and Anolli,2003; Oppenheim, 2000), and the online survey tool (Rowley,2014) was chosen as a suitable alternative to traditional paper based methods. The nature of the questions asked did not require expert knowledge, so militated towards a sample of the general population being selected. Survey respondents were all paid a small monetary sum for their participation.

Although it is not possible to legislate for the sample error it was possible to baseline the sample size, and the number of respondents required for the final questionnaire was calculated using statistical heuristics as being at least 150 (Hair et al., 2010) based on the number of constructs and indicators in the structural model. If, however, more than 300 samples were achieved the baseline could be relaxed (Tinsley and Tinsley, 1987; Floyd and Widaman, 1995). Therefore, the questionnaire aimed to process the maximum number of respondents that could be gathered to allow for any sample errors. The timescales used in all phases of data collection and the number of participants involved are detailed in the next sub section.

4.6.2 Data Collection Timescales

The collection of data for the research project was carried out in three phases, initial; pilot; and final data collection (Table 4.1). Each phase had differing objectives, with the overall aim of data collection being the collection of responses with high validity suitable for analysis.

Table 4.1 Data Collection Timescale

Phase	Research Method	Objective	Timescale	Sample size
Initial	Theory, Literature and Professional/ expert Review	Evaluate themes and contexts.	September 2017 – April 2018.	4
Pilot	Card Sort exercise	Determining Inter-rater consensus of the item stems and constructs. Construct validity.	2 weeks. April 2018	15
	Pilot online questionnaire	Item purification and scale validation, survey layout and timings.	2 weeks. June 2018	32
Final	Online questionnaire distributed to UK respondents.	Quantitative data for modelling, analysis, testing hypotheses and contribution.	2 weeks. November 2018	405 , after data cleansing

After collection of the data, the results were collated and analysed using the software tools detailed in the next section.

4.6.3 Data Analysis Tools

Different data analysis tools were utilised throughout the research, dependent upon the type of data collected and the objectives of the data collection exercise.

Data for the Card Sort exercise was captured by photographing the final layout of the cards as presented by each respondent. The data captured was transcribed to an excel spreadsheet for analysis. This was subsequently used in both a qualitative and quantitative basis for the Rater Identification (Section 5.2.5) processes. Additional notes relating to the data assessment and capture of qualitative data provided by participants about the layout and item clarification was manually recorded in the research notebook.

The ethically approved pilot survey was created using the onlinesurveys.co.uk (formerly Bristol Online) online survey instrument. This allowed flexibility of design and allowed quick updates in layouts to be made in preparation for the final survey questionnaire. The questionnaire data were downloaded from the website and stored in excel spreadsheets in university secured storage files. Feedback from the pilot survey was recorded manually or via email and transcribed into an excel spreadsheet.

The full survey data were collected by using the Qualtrics online survey platform. Qualtrics are a data provider that hold respondent panels these individuals were able to access and complete the questions anonymously. The provider was instructed to provide 400 respondents targeted at the general UK aged over 18, with respondents

evenly split between the three research context scenarios. As part of the contract the following data collection and cleansing services were also provided:

- Survey review, to ensure the questionnaire flow was correct.
- Technical Redirect setup, to screen out and ensure connectivity.
- Dedicated Qualtrics Project Manager to ensure quotas were met.
- Managed Soft launch, to field test the questions before a full release.
- Replacement of unusable data.
- Development of quality checks including attention filters and survey timings.

The raw data was downloaded from the website in excel spreadsheet format. These were imported to SPSS version 25.0.0 .sav files where the data were screened and cleansed. SPSS was applied to the analysis of descriptive, univariate and bivariate data analysis, and EFA analysis. Multivariate data analysis was carried out using AMOS version 25.0.0, to perform CFA and CB-SEM based statistical techniques based on the results of univariate and multivariate distribution normality testing methods described in **Chapter 6, Research Methods**.

4.6.4 Ethical Considerations

Ethical approval was sought and granted for each substantive stage of the research. Table 4.2 provides the outline detail of each ethics approval related to this work. The introduction of the GDPR required that the format and permissions required for Coventry University ethical processes was changed in May 2018, and the detail of the approvals incorporate these requirements.

Table 4.2 Ethical Approvals

CU Ethics Approval Number	Purpose	Date Valid From	Date Valid To
P80355	Data analysis and write-up phase	01/01/2019	30/09/2019
P71888	Full survey questionnaire	16/07/2018	31/12/2018
P70406	Pilot questionnaire	08/05/2018	15/06/2018
P64922	Card Sort Exercise	26/03/2018	28/05/2018
P61056	Literature search and desktop research	19/09/2016	30/09/2019

4.6.5 Data Collection Summary

The processes of data collection were planned and executed using the techniques described to ensure that the research data collected were collected and stored ethically in the correct format for analysis, and that the software tools used were suitable for the type of analysis required to fully investigate the research problem.

4.7 Methodology and Methods Conclusion

This chapter described the steps towards using the critical realist research paradigm. This process was outlined by describing the characteristics of the ontology,

axiology, epistemology and methodological components that a paradigm, or blueprint, that the research effort needed to follow. The most popular research paradigms used in the field of enquiry were also detailed prior to an analysis of the researcher stance. An assessment of the stance taken led to the choice and justification of the paradigm that was used to guide the methodology choices used in the research strategy.

The methodology was realised through the formation of a research strategy to investigate the problem, using both qualitative and quantitative research methods. These methods were delivered to produce an ethically sourced dataset that was suitable for analysis using the selected univariate and multivariate data analysis tools.

The logical research constructs defined in **Chapter 3, Conceptualisation** were subsequently assessed in the light of the methodology and used in the process of item generation and scale development operationalise the process of response measurement and hypothesis testing. This process is detailed in the next chapter, **Chapter 5, Scale Development and Item Generation**.

5. Scale Development and Item Generation

Chapter 3, Conceptualisation defined a conceptual structural model encompassing both the constructs and conjectured relationships between them that were relevant to the domains of trust and cybersecurity. The objective of the twin processes of item generation and scale development was to produce variables with which to operationalise and measure the model constructs in a manner consistent with the methodology choice and the rationale explained in **Chapter 4 Research Methodology Choice**.

5.1 Introduction

The process was to identify attributes and item parts that considered together encapsulated reliable measurement of each construct is known as item generation. The application of rules to measurement of the generated attributes was used to ensure that the construct definition was correctly captured by the measures (Churchill, 1979), and this process of measurement rule definition, generating and selecting items to form a scale to measure a construct is known as scale development.

Modification of the constructs, item generation and purification of pre-existing measures and scales required that a re-appraisal of the reliability and validity of the measures was carried out using the procedures suggested by Churchill (1979) to ensure that any prior scales were suitable for re-use in the research project and to

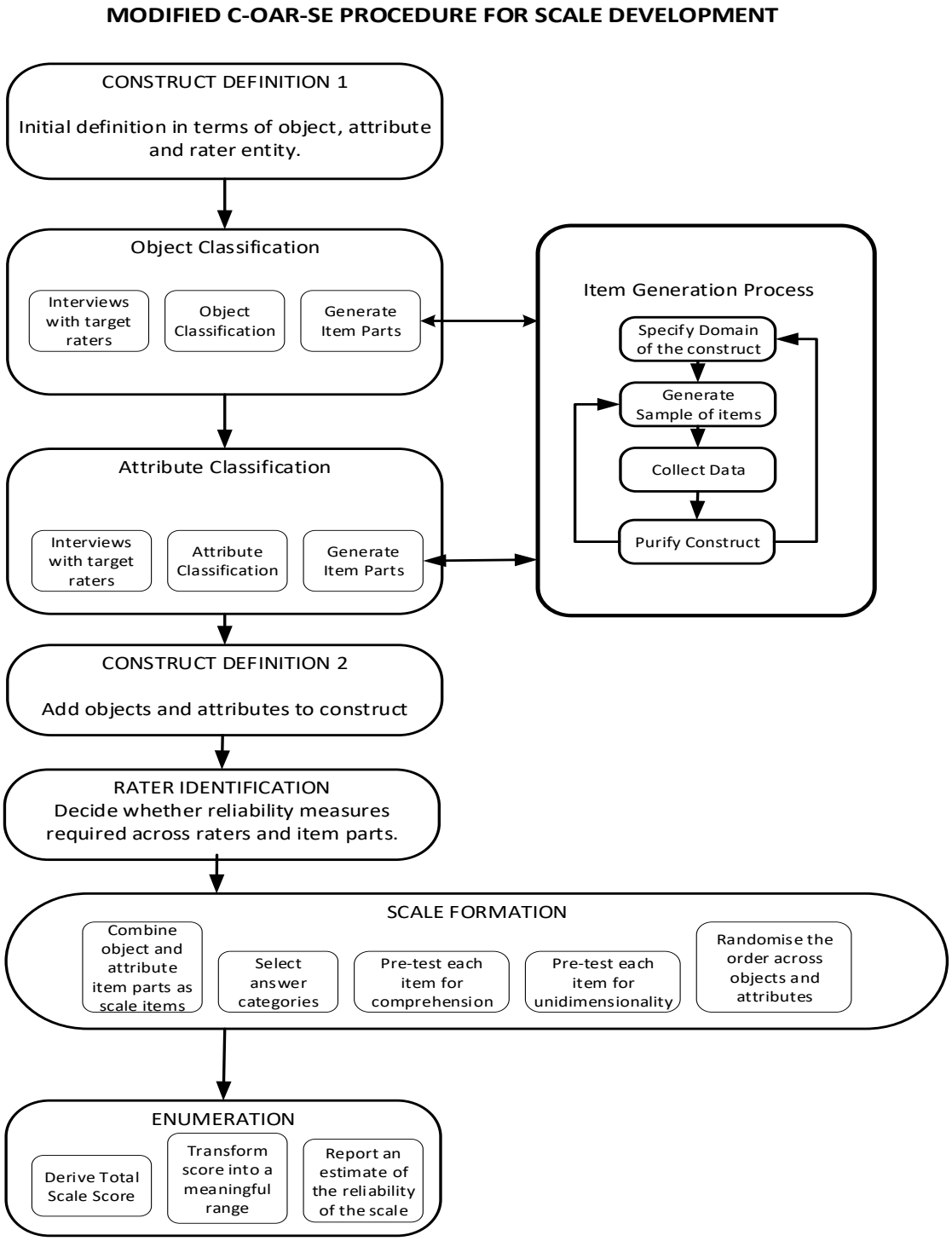
ensure that they retained their discriminant validity and relevance. The procedures employed in both item generation and scale development and validation were utilised to produce the measures and scales as detailed in the following sub sections.

5.2 Scale and Item Development

The iterative process of scale development with which to assess the measurement of constructs has been of academic interest across many fields of enquiry in the social sciences (Churchill, 1979; Anderson and Gerbing, 1988; Netemayer et al., 2004; Nunnally et al., 1967). Standardisation of the work of generating constructs and building measurement scales was achieved by using the Churchill (1979), and Rossiter (2002) frameworks to ascertain the consistency and validity of the scales and increase the reliability of research results measurement.

For the research constructs and indicators, the procedure employed to provide measurement scales was based on the C-OAR-SE (Construct definition, Object classification, Attribute classification, Rater identification, Scale formation, and Enumeration and reporting) procedure proposed by Rossiter (Rossiter, 2002). This procedure was modified to incorporate the item generation process proposed by Churchill (1979) to accommodate pre-existing items into the scale development process (Figure 5-1).

Figure 5-1 Procedure for Scale Development (After Rossiter, 2002)



The aim of item identification and generation was to produce a consistent system that assigned quantities to the attributes of the model constructs rather than directly to the construct itself, and scale development techniques were used to both refine and purify the items and to provide consistent measurement scales for the items. The application of the steps in this framework to the research is detailed in the following sub sections.

5.2.1 Construct Definition Stage 1

The constructs tested were conceptually defined to ensure that the definition could support operational measurement. The research model comprised of seven constructs, each of which measured a conceptually separate component. Constructs are factors that represent the phenomena of theoretical interest (Edwards and Bagozzi, 2000). Each construct is differentiated from the other constructs by means of attributes. Measurable and distinct attributes made it possible to rate or judge the construct. The outline construct attributes are detailed in Table 5.1.

Table 5.1 Outline Construct Attributes

Construct	**Item Constituents (Item Parts)**
Communication Quality	Message Relevance, Support, Calm
Delegation	Action, Goal Attainment, Acting in place of trustee
Outcomes	Feedback, Post hoc evaluation

Construct	Item Constituents (Item Parts)
Security	Information handling norms, congruence with customer expectation.
Trust	Confidence, Belief, 'knowing'
Reputation	Honesty, principles, care for trustees.

5.2.2 Object Classification

The defined conceptual construct definitions were classified according to their object category, and to the attributes that they were most closely identified by and on which the object was judged. The results are listed in Table 5.2.

Table 5.2 Object Classification

Construct	Object Classification	Meaning
Communication Quality	Abstract Collective	Connotative
Delegation	Abstract Collective	Denotative
Outcomes	Abstract Collective	Denotative
Security	Abstract Formed	Denotative
Trust	Abstract Eliciting	Connotative
Reputation	Abstract Formed	Denotative

The research constructs were classified into object types (Rossiter, 2002), namely concrete or abstract. Concrete constructs are those that are described nearly identically by all of the rater sample, for example, a chair. Abstract constructs are those that have different mental representations to different people, for example, good parenthood. The objects were also sub-classified as being collective (where the construct forms a census of its' associated attributes), formed (where the attributes suggest the nature of the construct), and eliciting (where the abstract construct relates to an internal trait or state that has external manifestations).

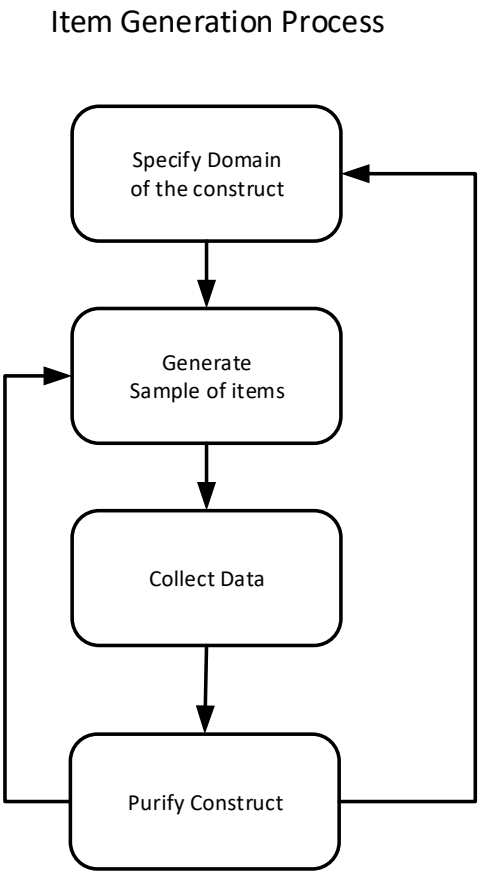
In line with the critique of the C-OAR-SE method (Diamantopoulos, 2005), an assessment of whether each construct is denotative (a sign of), or connotative (is implied by) of its' attributes is also included. This distinction is made to aid the interpretation of the constructs, as denotative variables are analysed in terms of what they include, and connotative variables in terms of what they mean. This had implications for measurement invariance between scenarios (Section 8.6.1), but did not affect the other phases of scale development. Having classified the object types the next step was to generate the attribute items to fully represent the constructs, detailed in the next sub section.

5.2.3 Attribute and Item Generation

For this thesis, the steps in the process for measurement item generation followed the first four steps of the suggested procedure for better measures suggested by Churchill (1979). The process excluded the calculation of Cronbach's

reliability scores as this was not judged necessary for established items. Item parts were allowed to be independent of constructs until the full questionnaire results were received. This sub-process that was used within used within the broader framework of the C-OAR-SE scale development process is outlined in Figure 5-2. Whilst using the C-OAR-SE procedure there is only one type of validity that is essential, that of content validity (Rossiter, 2002; 326). Content validity was ratified by expert agreement with domain expert raters checking constructs before the scales were developed, to help ensure that the proposed items rationally represented the construct in question.

Figure 5-2 Attribute and Item Generation Process (After Churchill, 1979)



The attribute item parts relating to communication quality, trust and reputation were derived from existing management literature relating to trust in the first instance. Task delegation attributes and items were drawn from machine trust research and multi agent systems (MAS) research to capture the machine-led nature of online processing. Outcomes was proposed as a new construct to reflect the union of machine output with the assessment of those outputs by way of communication feedback mechanisms.

Cybersecurity is relatively recent in a management context (Rothrock et al., 2018). This made it necessary to utilise pertinent literature and scales from related fields in the social sciences as guidance for item generation for new constructs relating to information security. That new items and constructs were added for security reflected the paucity of prior scales available in the cyber-psychology domain; in updating existing items to reflect the cybersecurity dimension of the constructs; and to acknowledge the influence of cross-contextual data breach concerns. Security items were gathered from organisational security research (Knapp et al., 2006) reflecting the values based concerns of the individual and the role of the trustee in assuring the success of delegation.

The initial item pool numbered over two hundred items. Items were dropped where they overlapped different constructs, were not relevant, or there was some ambiguity within the initially chosen item stems. Further expert consultation was used to reduce the item pool and to identify and combine related items into a single measurable item. The rationale for the inclusion or exclusion of all items was recorded

(**See Appendix A1**). The resulting candidate item pool was found to be valid on the grounds that *"If the sample is appropriate and the items "look right," the measure is said to have face or content validity"* (Churchill, 1979; 65), thus reaffirming the C-OAR-SE content validity criteria. The remaining fifty-six items were included in the card sort exercise that was used to further develop, purify and validate the constructs.

5.2.4 Construct Definition Stage 2

Having initially identified the constructs and their associated attributes and item parts a re-evaluation of the conceptual definition of constructs was important to ensure that they were unidimensional in scope, as measuring a single concept is both a critical and basic assumption of measurement theory (Hattie, 1985).

As discussed in the literature review (**Section 2.7**) trustworthiness has been conceptualised as a multi-dimensional construct based on the dimensions of ability, benevolence and integrity (Mayer et al., 1995). The thesis research model divides the latent variable of trustworthiness into the measurable facets of reputation (the exogenous component of trustworthiness), trust (an attribute describing whether an individual has belief in the trustee), and communication quality (an outcome of both trustworthiness and belief) in online environments. This differentiation of the concerns of trustworthiness was performed to achieve a more precise dimensionality of measurement of constructs, even though they were likely to display some co-correlation. Conceptualising cybersecurity constructs necessitated a focus on aspects of inter group security and organisational group (security) measurements. The

protective mechanisms as information security controls were chosen to reflect security concerns in trust formation. The delegation of tasks and achieving of outcomes is an essential feature of the transition of cognitive trust into behavioural manifestation (Schoorman et al., 2016). Delegation and outcomes were chosen to indicate the presence of the variables associated with the behavioural elements of trust.

These divisions of trustworthiness, security and behaviour into their hypothesised components was used to describe the identification of the constructs on the basis of attribute identification and to aid analysis of the contribution of this thesis that security and trust are related, a task that was made easier by a stepwise decomposition of the higher level constructs. The nomenclature used to describe the constructs was a reflection of the rater of the objects in question, and the method to ascertain the rater identification was based on a card sort detailed in the next sub section.

5.2.5 Rater Identification

The use of rater entity when applied to constructs (Diamantopoulos, 2005) requires that there is a degree of difference between the conceptualisation and operationalisation of constructs. Application of the rater identification method to the final questionnaires as per Rossiter, (2002) defined the constructs ‘as perceived by members of the UK general public’. However, to reach some consensus on the

attributes and content of the constructs it was necessary to rely on a card sort exercise utilising a smaller number of participants.

Table 5.3 Card Sort Participant Demographics

Participant ID	Gender	Age Group	Education Level	Occupation
1	F	18-24	Degree level	Civil Servant
2	F	25-34	Degree level	Teacher
3	M	35-44	Degree level	Charity Worker
4	M	35-44	Postgraduate degree	IT Specialist
5	M	25-34	Postgraduate degree	Cybersecurity Specialist
6	M	25-34	Postgraduate degree	Cybersecurity Specialist
7	F	35-44	College study	Administrator
8	F	18-24	Postgraduate degree	Lecturer
9	M	18-24	Degree level	Student
10	M	25-34	Postgraduate degree	Lecturer
11	F	55-64	Finished School	Administrator
12	F	18-24	Degree level	Student
13	F	25-34	Postgraduate degree	Student
14	F	35-44	Finished school	Shop Assistant

Participant ID	Gender	Age Group	Education Level	Occupation
15	M	45-54	Finished School	Car mechanic

The card sort exercise was carried out with fifteen respondents, recruited as a convenience sample. Of these respondents eight were selected from the research community at Coventry University and the other seven respondents were drawn from the general population. The general population sample included practitioners working in cybersecurity, software systems design and civil servants with domain knowledge in freedom of information requests (Table 5.3). The inclusion of non-expert raters was to ensure that the understanding of the abstract constructs was consistent with the skill levels of potential questionnaire participants and to ensure that the connotative and denotative meanings of the constructs were widely held, thus reducing researcher bias by misclassification (Boeschoten et al., 2018). This exercise also contributed to the convergent validity by helping to affirm the uni-dimensionality of the constructs employed.

The card sort exercise was also used to reduce the item pool from fifty-six to thirty-eight items, based on the ratio of items scored in each construct. The raw rater count for each item relevant to a particular construct was calculated, and the most popular choices for each were chosen as being typical indicators for that construct. The card sort thus provided an independent measure of construct validity where prior scales were used. This resulted in the table of constructs and items that were incorporated into the measurement model as included in Table 5.4.

Table 5.4 Card Sort Results

Construct	Count	Item
Security	8	I feel that the organisation appears to value the importance of security.
	7	The organisation should protect my assets and information from cyber threats and their effects.
	6	Information security is a key normal behaviour shared between myself and the organization.
	5	I am unable to influence the presence of threats inherent in the task.
	4	I have the possibility of redress in the event of task failure due to cyber threat.
	1	I feel sure that the use of online systems is appropriate to this task.
Confidentiality	11	Data privacy is more important to me than data sharing.
	10	The organisation should not use personal information for any purpose unless it has been authorized by the individuals who provided information.
	8	It concerns me when I see my personal preferences used in advertising.
	8	Information I have given in one context should not be used in an unrelated context without my permission or knowledge.
	6	My relationship information should be protected when it is shared, transmitted or stored.
	4	The authorised parties that have relationship confidential information are entitled to infer or draw conclusions based on our relationship.
	3	I have confidence that my information is destroyed after use, or at my request.
Reputation	13	The organisation has a reputation for looking after its customers
	12	The organisation has a reputation for being honest
	11	Sound principles seem to guide their behaviour
	4	I feel that the trustee cares about me
	2	The feedback I receive from the trustee is constructive in helping me make improvements
	1	They know what needs to be done
	1	Identification with trustee as part of group
Trust	7	I trust that the organisation would keep my best interests in mind when dealing with information.
	6	I believe that the information privacy assurances offered by the organisation will be honoured.
	6	I would be willing to let x have complete control over my online transactions.
	6	XX is always honest with me
	4	Same values – different values
	4	XX makes every effort to address my needs
	3	I believe that being associated with XX reduces the uncertainty I face
	2	My sense of belonging is shared with others.

Construct	Count	Item
Delegation	12	I believe that delegating the task will achieve my task goal
	8	I can trust the delegated agent to act in my place.
	5	I trust the trustee enough to allow him/ her to delegate the task to another person/ Information system
	5	The agent has a great deal of autonomy on this task.
	3	It is easy to evaluate the delegates' skills accurately.
	2	I am /am not aware that the information is being dealt with by an external agent.
Outcomes	8	Achieving the transaction gave me the confidence to engage with the trustee again
	8	I am able to give objective feedback to the service provider.
	7	The trustee has informed me of other customers that have seen positive outcomes from their association.
	4	I am able to assess how the trustee dealt with situations similar to mine.
	2	My opinion of the trustee has increased based on our history of transactions
	1	I was able to assess the before and after state of the transaction with confidence
	1	The organisation makes good-faith efforts to address most customer concerns.
Communication Quality	8	I receive relevant and timely notifications from the XX
	8	XX will deal calmly and efficiently with any unexpected events.
	7	Communication from XX happens in a predictable manner.
	4	Interaction with XX is generally constructive and supportive.
	2	XX always contacts me via the same medium (e.g. email, text message, phone call, letter)

Based on the results from the card sorting exercise the items were reworded into context specific questions in line with the scenarios chosen. In addition, a set of introductory demographic and attitude based questions were created to record the possible moderating effects of gender, age group, highest education level, prior cybersecurity awareness, privacy sensitivity attitude, online behaviour preferences and trusting attitude.

It is known that cybersecurity is contextual (Nurse et al., 2011) and the inclusion of scenario contexts were incorporated into the survey questionnaires to account for the variation of perceptions and attitudes across three areas of online concern that

were included in media stories about cybersecurity in the months preceding the survey. The scenarios chosen were retail shopping, online banking, and the use of electronic health records for secondary research uses (**See Section 3.2.9**). The scaling of the items for measurement and scoring purposes was achieved by using methods of scale formation, which are detailed in the following sub section.

5.2.6 Scale Formation

Scale formation in C-OAR-SE is a matter of putting together object item parts with their corresponding attribute item parts to form scale items (Rossiter, 2002). A standard five point reverse scored ordinal Likert scale was adopted for all of the question items. Some of the original question items were originally published as seven item scales, or were part of a wider selection of responses, in which case the original question was reworded to allow for a five scale type to be used. Guidance was followed on the use of five scale items as the best fit for the number of psychological discriminations made by consumers (Miller, 1956). Of the pre-existing items, the majority were originally scaled as five item choices. The final choice of five point scaled item parts that characterised the demographic, attitudinal, and construct objects measured and details of prior provenance are included in Table 5.5 along with the questionnaire number that was allocated. To avoid common method bias (Mackenzie and Podsakoff, 2012) construct questions were randomly allocated a position in the questionnaire.

After production of the scaled and contextualised questions the enumeration and reporting characteristics of the questionnaire were evaluated, and this process is described in the next sub section.

Table 5.5 Constructs, Item Stems and Provenance

Demographics and Attitudes		
The following items were collected from all of the questionnaire participants.		
Item Stem	**Item Source**	**Questionnaire Number**
Age Group	Malhotra et al.,2004	2
Gender	Smith ,1996	3
Education	Smith ,1996	4
Media exposure	Pavlou and Dimoka,2006	5
Trusting Preferences	Myers et al.,2003; Gefen,2000	6
Privacy Attitude	Malhotra et al., 2004	7
I generally trust other people	Rotter, 1967	8
I generally have faith in humanity	Rotter ,1967	9

Communication Quality

The communication between the trustee and trustor is dependent upon communication that facilitates trust in the co-creation and sharing of vulnerability and task information.

Item Stem	Item Source	Questionnaire number
I receive relevant and timely notifications from the provider	Jarvenpaa and Leidner, 1999	49
The provider will deal calmly and efficiently with any unexpected events.	Jarvenpaa and Leidner, 1999	50
Communication from the provider happens in a predictable manner.	Jarvenpaa and Leidner, 1999	53
The provider always contacts me via the same medium (e.g. email, text message, phone call, letter)	Jarvenpaa and Leidner, 1999	52
Interaction with the provider is generally constructive and supportive.	Jarvenpaa and Leidner, 1999	55
When required there is two-way communication between myself and the provider.	New Item	54

Delegation

The act of delegation to another party is where control of a task or tasks is ceded to that party in order that they are able to act on behalf of the trustor.

Item Stem	Item Source	Questionnaire number
I trust the provider enough to allow him/ her to delegate the task to another person/ Information system	New Indicator	14
I believe that delegating the task will achieve my task goal	Castelfranchi,2001	15
The feedback I receive from the provider is constructive in helping me make improvements	Colquitt,2011;Tajfel and Turner, 1979	17
I can trust the delegated agent to act in my place.	New Indicator	27
The agent has a great deal of autonomy on this task.	Adapted from Mayer , 1999	34

Outcomes

The outcome of a task is the evaluation of how it works out. It is the consequence or implication of the delegated actions of the trustee.

Item Stem	Item Source	Questionnaire number
I am able to assess how the trustee dealt with situations similar to mine.	New Indicator	16
The trustee has informed me of other customers that have seen positive outcomes from their association.	Pavlou, 2003	25
Achieving the transaction gave me the confidence to engage with the trustee again	New Indicator	26
I am able to give objective feedback to the service provider.	New Indicator	33

Information Security

Security is defined as being the state of being free from danger or threat (OED, 2019), and includes safety from criminal or military threat. Information security is conceptualised as being a way of protecting information so as to prevent such threats.

Item Stem	Item Source	Questionnaire number
I feel that the organisation appears to value the importance of security.	Adapted from Knapp et al., 2006	11
Information security is a key normal behaviour shared between myself and the organization.	Adapted from Knapp et al., 2006	19
The organisation should protect my assets and information from cyber threats and their effects.	Anderson and Agarwal, 2010	30
I am unable to influence the presence of threats inherent in the task.	Adapted from Probst, 2001. Job Security Index (JSI)	42
I have the possibility of redress in the event of task failure due to cyber threat.	Adapted from Probst, 2001. Job Security Index (JSI)	45

Trust

Trust is the confident expectation that a trusting party will engage with other(s) to effect a net positive outcome in situations where risk, vulnerability or uncertainty are acknowledged or present. (Section 2.3.2). Trusting belief is the acceptance that the following statements are believed to be true without proof.

Item Stem	Item Source	Questionnaire number
The organisation would not knowingly do anything to harm me.	Adapted from Mayer and Davis, 1999	18
I have confidence that my information is not modified without consent and is destroyed after use, or at my request.	New Indicator	48
I know that my information is safe and access is limited only to authorised personnel.	New Indicator	28
The organisation keeps my best interests at heart when dealing with my information.	Malhotra et al. ,2004 - IUIPC	32
I believe that the information privacy assurances offered by the organisation will be honoured.	New Indicator	44

Reputation

"The overall evaluation of a company over time based on direct experience and any other form of communication and symbolism that provides information about a firm" (Gotsi and Wilson, 2001:29), and is based on the trustworthiness attributes that are externally displayed by the trustee.

Item Stem	Item Source	Questionnaire Number
The organisation has a reputation for being honest	Doney and Cannon, 1997	12
Sound principles seem to guide their behaviour	Sekhon et al., 2014	23
My opinion of the trustee has increased based on our history of transactions	New Indicator	24
The organisation has a reputation for looking after its customers	Sekhon et al., 2014	38

5.2.7 Enumeration and Reporting

The item stems were contextualised into questions that were incorporated into an online pilot questionnaire, which was completed by thirty respondents. The production of the pilot questionnaire was essential for item and measure purification and assisted in triangulating the understanding of the objects, attributes and item relationships. This exercise prototyped the wording and outline timings of the operational constructs and the structure with which they had been created.

The pilot survey participants were a convenience sample drawn from the Centre for Business in Society at Coventry University. In-depth questionnaire feedback was actively sought from the researcher participants of the pilot questionnaire by follow up email. Seven of the respondents volunteered detailed feedback that was incorporated into the final questionnaire design (Table 5.6 Pilot Questionnaire Feedback Items), and a further five respondents were followed up personally for feedback on the experience of, and the layout of the online questionnaire instrument. The distinct transcribed feedback items are detailed in Table 5.6, with actions taken to remedy noted.

Table 5.6 Pilot Questionnaire Feedback Items

Feedback Item	Comment	Rationale / Action(s)
1	Use scales of 1=Strongly Agree to 5=Strongly disagree to code the responses	The responses were coded in this format for data analysis.
2	Consider removing anchors for options agree and disagree if possible	The online survey tool used for the pilot did not permit this. However, this suggestion was carried forward to the final questionnaire.
3	Clarify, or re-clarify the meaning of EHR to the reader, or just use health records as easier to understand	Health record or electronic health record was used. In a health context, an EHR has a special meaning as a fully integrated records system that is only partially adopted in the UK. The term 'health record' is used in the item to indicate use of an information system by the practitioner.
4	Typos in questions 14,15 of the health questionnaire	Corrected.
5	Question 16 has a transaction that doesn't seem to fit the situation. "Allowing the healthcare provider to update transactions electronically gave me the confidence to engage with the same provider again." Reword this?	Reworded to: "Allowing the healthcare provider to update my health records electronically gave me the confidence to engage with the same provider again." Preserves the item stem meaning of a transaction within a health context
6	The question on the first page (preliminary questions) that asked "I have a preference towards..." Is the purpose of this question to determine whether people are more trusting in dealing with people in a face-to-face environment or online? The answers didn't seem mutually exclusive (e.g. it is possible to have a preference for dealing with people you have experience with and also evaluate decisions logically and rationally, at least I feel it is).	The question is a forced preference question used in prior work Mallach, 2000; Myers, 2003 used to differentiate respondents with a Sensing, Intuition or Thinking preference. Analysis of respondent type links person type to the relative importance of constructs. Utilised in the Myers-Briggs personality classification types.
7	"I trust the bank enough to allow it to delegate the task of fulfilling my instructions to another person or information system" I wasn't very clear at first what kinds of tasks the bank would have any reason to delegate to another person. I think the next question clarifies this a bit by having in brackets (e.g. to a payment processing system). Perhaps consider adding such a clarification to this question too?	Clarification added to keep question format consistent.
8 (2feedbacks)	"The feedback I received from the bank is constructive in helping me make improvements." What kind of feedback do you mean? My bank doesn't really	Some banks, and the UK Government (through the midata initiative) encourage customers to use their own data to gain insights into their

Feedback Item	Comment	Rationale / Action(s)
	give me any feedback, just the occasional bank statement... Also, what kinds of improvements? To the way I manage my finances?	behaviour, either through downloading personal data, showing customers visually how they spent, or allowing comparison to 'similar' customer profiles. Revised question to "The information I receive from the bank is constructive in helping me manage my finances."
9 (2feedbacks)	"The bank has specialised capabilities that can increase my performance". Increase my performance in what? Do you mean the interest I earn on my assets or something? I've never done any type of investing or stock trading or whatever so I don't tend to think of my finances in terms of "performance".	Specialism relates to domain competence (Doney and Cannon, 1997), and the strength of trust based on specialisation. Reworded to "The bank has specialised capabilities that can increase my financial wellbeing".
10	Adding a "Don't know/not applicable" option. For some of the questions I really struggled to know what to answer as the question didn't really feel applicable to the way I do my online banking. For most of these I just answered "Neither agree nor disagree" but that has a slightly different meaning than "not applicable".	Item stems are generalised over different scenarios some questions may not fully correspond to a scenario. Analysis will utilise both strong and weak responses as part of the structural model. No modification made.
11	The questions are long and therefore for your bigger wider survey - to keep someone engaged you might need consider offering them an entry for a prize or pay them a voucher to do it.	As part of the data collection payment was used to ensure participation, and a discussion of this choice is in the Research Methods chapter.
12	You position the privacy propensity and trust propensity questions up front and I wonder will that introduce confirmation bias to your questions which follow? Should it be at the end? Just a thought.	The self-evaluated propensity positions are used to frame the analysis answers, rather than to guide the responses.
13	It would be nice to tell me how long the survey will take and a percentage completed as I go through it. This will also keep respondents engaged.	An estimate of 10 minutes for completion and an online completion percentage chart was included into the final design.
14	You use the terms cyber-threat and information security. You don't define these - and cyber-threat is very subjective/unknown to the public so it might be worth explaining. I think most lay people will think 'hackers' but it is also 'downtime' and systems unavailability and ransomware etc.	By design. Respondents provide their subjective responses to questions without needing to know or reflecting on the type of differentiated threat, as they do in normal online interaction.
15	"Compared to others, I am more sensitive about the way online companies handle my personal information" can a subject really compare themselves to others in this manner. I don't know how sensitive you are or anyone else is..... I felt this almost impossible to answer.	By design. The perceived sensitivity is analysed as a co-variate factor in the responses.

Feedback Item	Comment	Rationale / Action(s)
16	"I know that the personal information I give to the bank is kept anonymous and safe". Information is rarely kept anonymous (this is a term used in GDPR so I would not use it. I think what you mean here is “I know that access to my information is limited to only authorised personnel” or something to that affect.	Reworded to “I know that my information is safe and access is limited only to authorised personnel”. To avoid confusion with the legal definition the research seeks the drivers of privacy rather than the mechanisms of enacting it.
17	"The bank should protect my assets and information from cyber-threats and their effects". The bank legally has to do this in order to get a license to operate from the regulator. So it is not optional or down to the consumer.	Not modified. Although the legal obligation may exist, this does not mean it reflects the attitudes of respondents.
18	"The bank makes rules and regulations, sets limits to activities and enforces the rules and limits to our interaction". The bank doesn’t make regulations, the central banking authority does. The bank has to follow and implement those regulations or else it doesn’t get its license to operate.	Reworded to avoid confusion with banking vocabulary to "The bank makes rules about our interactions, sets limits to activities and enforces the rules and limits to our interaction". Also reworded for health care scenario question to "The healthcare provider makes the rules about our interaction, sets limits to activities and enforces the rules and limits to our interaction".
19	"Information I have given to the bank in one context should not be used in an unrelated context without my permission or knowledge". GDPR says that a data controller cannot do this, so essentially you are asking the respondent do they agree with the law.	Not modified. Responses will help to determine if the law reflects attitudes and perceptions of data usage. Retained to keep items consistent across all sectors, not only the banking scenario.
20	"It would concern me to see my health information used in targeted advertising by the healthcare provider (e.g. notifications of new/ relevant services)" do you mean 'without my consent'? It would not concern me if it was with my consent.	Reworded to "It would concern me to see my health information used in targeted advertising by the healthcare provider (e.g. notifications of new/ relevant services) without my consent”
21	"The healthcare provider has specialised capabilities that can increase my performance". Would this include a prescription for performance enhancing drugs?	Reworded to "The healthcare provider has specialised capabilities that can increase my health and wellbeing".

One of the additional aims of using the pilot study was to ensure that sufficient discriminant validity of the items was retained, and the provision of summated multi-item scales of construct measurement provided the discriminant validity required, as opposed to relying on single question scales (Churchill, 1979). The five point scale selected reflected the majority of the existing scales, but is lower than the recommendation of an eleven point scale (Diamantopoulis, 2005). This loss of precision was not reflected in the measures of reliability, as subsequently calculated in Cronbach alpha and Item loadings data, and resultant stability of the scale in this application. The measurement of the Cronbach alpha values (**Section 6.3.4)** provided nomological validity that the construct being measured related to measures of constructs that are theoretically related to it in ways predicted by the theory (Sekhon et al., 2014).

The feedback was incorporated into the wording of the final questionnaire items, an example of which is included in **Appendix A2**.

5.2.8 Scale Development Conclusion

The observed values obtained by measurements are composed of the true value, any systematic sources of error, and random sources of error. The validity of such methods relies upon reliably measuring the characteristics of the 'true' score. Measuring true values depends on how much of the observed variation is composed of attributable errors (Churchill, 1979). The use of the C-OAR-SE methodology to

conceptually define and refine the measurement of the research model added validity and reliability into the investigation of the problem. This process incorporated several stages of construct, object, attribute, item part generation, rater identification and scale development into developing the conceptual products of the model into operationally viable questions.

The process of item generation produced considerably more items than were used in the final construct definitions used for analysis. An initial pool of 195 questions (Appendix A1) were streamlined to the final 38 questions (Appendix A2). Although dropping items involved a series of processes to increase the purity of the scales in measuring the required model variables it also brought additional choices that the researcher had to adjudicate on. Initial processes allowed item reduction through expert and literature identification of repeating or similar items, and were used to differentiate between questions that would be better suited to formative rather than the reflective scales that were used (Diamantopoulos, 2001). Rater identification was used to further reduce the item count, with some items strongly identifying with constructs. Other items did not identify with a single item, and needed to be discarded to ensure that the developed scales provided the discriminant validity required for measurement purposes.

Following a structured methodology assisted in assuring that observed scores used in analysis represented the true reality as closely as possible. Allied to the aim of obtaining ‘true’ data, measure reliability is also important in making the findings reproducible by other researchers and was a necessary ingredient for determining the

validity of the research. The method followed did not rely on upfront measures of indexes of reliability that were utilised after the final data collection to quantify the content validity as part of EFA and CFA analysis. The techniques and results of reliability analysis are detailed in **Chapter 6, Research Methods and Chapter 8, Multivariate Data Analysis** respectively.

5.3 Scale Development Chapter Conclusion

Although many of the research constructs included in the model were seeded from prior research, the introduction of the new variables (Information Security and Outcomes) required definition, classification, item generation and scale development to be carried out to ensure that the constructs were adequately identified with attributes, and that the item parts chosen were strongly related to the constructs in question. The approach taken allowed a flexibility of approach by considering more items before crystallising the construct definition based on item loadings and measurement reliability. Overall, 42% of the final measurement indicators were based on measures that had not previously been used with the same wording in previous research, so the processes reflected an almost even balance between new item generation and scaling or re-scaling existing items. The item generation, scale formation and item purification methods were chosen to maximise the validity of the measures, the constructs and the measurement model. Utilising the mixed qualitative and quantitative research techniques outlined in this chapter to generate items and to create and purify scales of measurement it reduced the potential for, and size of estimated error conditions based on the data that was subsequently collected.

The research methods and techniques employed relied on the scaled items that have been outlined in this chapter. Undertaking scale development before implementing the research methods ensured that the analyses were based on correctly generated and scaled reliable data that marked the research as content valid and reproducible. An outline of the Research Methods that were utilised to transform the raw data collected into statistical evidence are detailed in the next chapter.

6. Research Methods

Following the previous chapter covering the choice of research methodology, and given that the research process follows from the paradigm choice (Burrell and Morgan, 2017), the research methods employed in this thesis were chosen to guide and ground conducting the research by providing the rules, systems and procedures against which the claims of the research were gauged (Frankfort-Nachmias and Nachmias, 2007) using the chosen critical realist paradigm.

6.1 Introduction

The methods were used to assemble evidence to support or refute the research model and contributions to theory and were critical for the justification of the claims of this thesis to represent the underlying reality of the problem space. The research design connected the data to the causal inferences asserted by the researcher through the use of logical methods. In the case of the current thesis, this is that the cognitive and behavioural attributes of trust display patterns that do not fall randomly. They are clustered around, or are influenced by the organisational security and information confidentiality offered in digital environments.

The methods added rigour to the research processes by ensuring that the data collection and analysis followed a logical progression of routines. Each of the routines was followed to provide precise inputs and relevant outputs to the following stages of

the research. (Table 6.1 Research Methods Summary). To transform the chosen methodology into a process that delivered on the aims of the research the research methods used were implemented as an integrative strategy of scientific method to govern the standards employed in the item generation, scale development, data collection, descriptive statistics, and the multivariate data analysis phases. Following data collection, univariate and multivariate quantitative statistical techniques produced numerical outcomes of evidence. The techniques applied, and their application to original data sets has considerable depth of prior work in the fields of psychology, management and information systems research. These methods, and their descriptions and utilisation in the analysis process are detailed in the following sections of this chapter (Table 6.1)

Table 6.1 Research Methods Summary

Section	Technique	Methods
Descriptive Methods Section 6.2	Descriptive statistics	• Central Tendency • Variance • Standard Deviation • Kurtosis and Skewness • Outlier Detection
EFA Methods Section 6.3	Exploratory Statistical techniques	• Factor Analysis • Communality • Rotation • Reliability
CFA Methods Section 6.4	Confirmatory Statistical techniques	• Multi-collinearity Detection • Tolerance and VIF • Item loading • Factor Correlation • CR and AVE
SEM Methods Section 6.5	Structural Equation Modelling Techniques	• Model Testing • Model Recursion
SEM Model Fitting Section 6.6	Model Fitting measures	• Model Fitting and indexes
Model Stability Methods Section 6.7	SEM model stability techniques.	• Context Modelling • Measurement Invariance

Section	Technique	Methods
Moderation and mediation Methods Section 6.8	Mediation and moderation.	• Mediation Analysis • Moderation Analysis • Path Analysis

6.2 Descriptive Methods

The univariate normality of a distribution is generally characterised by the mean, variance, standard deviation, skewness and kurtosis of a dataset. Additional data screening for data outliers was also performed. These statistical tests formed the foundation of the assessment of univariate normality outlined in **Chapter 7, Descriptive Data Analysis.**

6.2.1 Measures of Central Tendency

For all variables the central tendency measure of arithmetic mean was calculated. The mode and median values were also calculated, and are reported only where they influence the analysis in terms of understanding the deviation of a measure from a normal distribution. Minimum and maximum values were recorded in the statistics to indicate the range of values encountered. Where responses did not include all possible values in the scale range these variables are noted, and the implications of the reduced range on the analysis are indicated.

6.2.2 Variance Indicators

The sample variance of a variable is expressed as the square of the deviation between a value and the mean of the sample set from which it is taken. This can be mathematically expressed as:

$$s^2 = \frac{\sum(X - \bar{x})^2}{n - 1}$$

Where X represents the sample value, $\bar{x}$ is the sample mean and n is the number of samples.

The F-statistic is a test for the null hypothesis that two populations possess the same variance. The F-statistic is the ratio of the variation between group sample means divided by the variation within the samples. If the null hypothesis is true, then the value of the F-statistic will tend towards one. The F value is reported alongside a significance value of <0.05 (Wasserstein and Lazar, 2016) below which threshold it is considered that there are significant differences in variation between the groups.

Levene's test is is an inferential statistic used to assess the equality of variances for a variable calculated for two or more groups. It tests for the null hypothesis that two populations display homogeneity of variance (that they display homoscedasticity). The resulting p-value should have a value of <0.05 (Wasserstein and Lazar, 2016) resulting in the rejection of the null hypothesis of equal variances and it is concluded that there is a difference between the variances in the population.

6.2.3 Standard Deviation

The sample standard deviation is mathematically expressed as:

$$sd = \sqrt{\frac{\Sigma(X - \bar{x})^2}{n - 1}}$$

The standard deviation is the square root of the variance and represents how spread out the numbers are in a distribution. Standard deviation aids the interpretation of how severely the deviation of values from normality are when used in conjunction with other measures, including the variance, skewness and kurtosis aid the statistical description of a distribution curve.

6.2.4 Kurtosis and Skewness

Kurtosis and skewness are terms used to describe the way in which a data distribution deviates from a bell-shaped normal distribution curve. Kurtosis is a term used to describe how peaked or flat a distribution is when compared to a normal distribution. A peaked distribution, where observations are bunched together when compared to a normal distribution is described as being leptokurtic, whereas a distribution that is flattened can be described as platykurtic (Hair et al., 2010). Kurtosis is a measure of the tail extremity of a distribution, and reflects the presence of outliers in the distribution, or the propensity of a distribution to produce outliers (Westfall, 2014).

Skewness describes how balance the values were, with values predominantly to the left of centre described as showing positive skew. Conversely, a distribution where the values tend to the right of centre are described as having negative skew. Statistical tests of skewness and kurtosis (z-scores) were calculated, and if the values exceeded (±) 2.58 for skewness and (±) 1.96 for kurtosis then the distribution could be said to be non-normal with respect to that characteristic (Hair et al., 2010).

6.2.5 Outliers

An interval Likert scale was used in the collection and variable scoring, with respondents opinions elicited on the items on a common five point structured scale with a minimum score of 1 (Strongly Disagree) and a maximum score of 5 (Strongly Agree). Demographic data were collected as respondent self-reported classifications from a mandatory list. Therefore, the data collected were less prone to extreme univariate outlier data than if a freely scored open ended series of questions had been asked.

6.2.6 Descriptive Methods Summary

Using the statistical methods described in this sub section the indicators of normality and non-normality were calculated to assess whether they displayed sufficient proximity to normally distributed variables to be included as part of the multi-variate data analysis.

6.3 Exploratory Factor Methods

Exploratory Factor Analysis (EFA) is a technique widely used and applied in social sciences (Osborne, Costello and Kellow, 2005). The analysis was carried out on a Factor Analysis (FA) rather than a Principal Component Analysis (PCA) basis as the emphasis of the analytical work was on factor generation from a priori known variables, rather than reducing the number of variables required, one of the relative advantages of using the alternative PCA method. EFA techniques originate from the Common Factor Model (Thurstone, 1931) and these methods were used to identify common factors to specify a parsimonious measurement model using a reduced number of latent variables.

6.3.1 Factor Analysis

Empirical support for the number of factors extracted for analysis was based on the latent root criterion and a priori criterion selection. Latent root criterion maintains that any individual factor should account for the variance of at least a single variable if it is to be retained for analysis. With each variable accounting for a value of one towards the total eigenvalue, only the factors that have latent roots or eigenvalues over one are considered significant (Hair et al., 2010).

Using a priori criterion the researcher knows how many variables to extract before conducting the factor analysis, and the computer is instructed to stop when the required number of factors are obtained. The theoretical justification for the stopping rule becomes the criterion for extraction.

6.3.2 Communality

The sum of the squared factor loadings, or communality, shows the amount of variance in a variable that is absorbed when two factors are considered together. Communality size is useful for assessing how much variance has been accounted for in a factor.

Assessment of the communality reveals which variables have more or less in common with all other variables included in the analysis. Although there are no statistical guidelines, modest communality of >0.5 is generally accepted as being sufficiently high to proceed with factor rotation methods (Hair et al., 2010).

6.3.3 Factor Rotation

The purpose of factor rotation is to simplify the factor structure and produce factors that are more meaningful by reducing the ambiguities that are present within the non-rotated factors obtained from the factor extraction process. This is done to relate the extracted factors to theoretical entities and can be achieved by using varimax methods where the factors are thought to be uncorrelated (or orthogonal), or by using oblique rotation methods like direct oblimin where the factors are suspected to be correlated (Vogt and Johnson, 2011). Rotated factor solutions redistribute the variance from the earlier factors to later ones with the aim of simplifying the structure (Hair et al., 2010). Rotation involves rotating the factor axes, or dimensions, identified in the initial extraction of factors, to obtain simple or interpretable factors (Corner, 2009) for analysis.

6.3.4 Reliability Analysis

A measure is said to be reliable when *"independent but comparable measures of a construct agree"* (Churchill, 1979), and the most commonly reported estimate of score reliability is Cronbach's coefficient alpha, a measure of internal consistency reliability. Constructs that display a high degree of internal consistency provide an assurance of measurement consistency that contribute towards the validity of the research model. Higher reliability scores reduce the level of variance introduced due to random error and in doing so increase measurement accuracy, strengthening the validity of the research.

The coefficient is calculated as one minus the observed variance due to random error, with values of 0.6 to 0.7 being deemed the lower limit of acceptability for reliable construct measurement (Hair et al., 2010), with values above 0.7 indicating a good fit (Nunnally and Bernstein, 1994). Measurement of Cronbach alpha values provide nomological validity that the construct being measured is related to the measures that are theoretically related to it (Sekhon et al., 2014). Reliability and validity are closely related as the research cannot be considered to be valid unless it is reliable (Tavakol and Dennick, 2011).

6.3.5 EFA Methods Summary

The EFA methods of factor analysis, communality, factor rotation and reliability analysis outlined in this section were used to relate the data obtained to common factors. The importance of using common factors in analysis is to permit the structure

of the underlying data points to be related to the theoretical constructs in the research model, and to give assurance that the reliability and correlation between and within the factors is sufficient to use these common factors as proxy measures of the research constructs themselves.

6.4 Confirmatory Factor Analysis

Confirmatory Factor Analysis was used to establish correlation between the constructs used in the structural model, and to ensure that the measurement model was of sufficient validity to accurately reflect the constructs that it supported.

It has been noted that there is rarely a clear-cut distinction between exploratory and confirmatory investigations (Anderson and Gerbing, 1988; Jöreskog and Sörbom, 1984). The research model was based on prior theoretical and empirical research carried out in related fields, the researchers' experience in the area of cybersecurity management, and expert opinion gained through discussion. This domain information was evaluated and synthesised by the researcher prior to proposing the model for investigation. Due to the balance of theoretical over exploratory research considerations CFA was chosen as the primary method of factor analysis.

CFA is a suitable analysis technique for data where the constructs were composed of observed variables that were broadly normal in distribution. The normality of the data were determined by the descriptive statistics presented in Chapter 10, Descriptive Statistics. The methods used were implemented to provide confirmation of the characteristics and nature of the factors that were identified as

part of the exploratory methods outlined in the previous section. Details of the confirmatory techniques used are introduced in the following section.

6.4.1 Multi-Collinearity Detection Methods

The simplest test for multi-collinearity in a dataset is when the bivariate correlation between constructs is high, generally 0.9 or above (Hair et al., 2010). Multi-collinearity is a case of empirical under-identification (Kenny, 1979), and can cause difficulties when evaluating the covariance between highly correlated constructs due to insufficient separation between the measures of one variable and another. High levels of multi-collinearity (with correlation values above 0.85) can result in biased analysis due to the exaggerating effects of multiple factors that may not be sufficiently discriminated (Kline, (2005), although a certain degree of correlation was expected between the factors, as this is often the case in social sciences (Costello and Osborne, 2005). Where multi-collinearity is suspected, there are generally two options, the variables can be removed from the constructs, or they can be merged into a single variable where the redundancy is suggested (Kline, 2005). The squared multiple correlation of the constructs (R^2), which calculated the percentage variation to the total variation was also assessed to ascertain how closely the observed values fitted to the constructs that represented them.

6.4.2 Tolerance

Tolerance, calculated as one minus the squared multiple correlation ($1 – R^2$) is the amount of unique variance in a dependent variable that is not explained by all

other independent variables, and is considered to be a better indicator where multiple variables are used to show pairwise correlations more clearly. Values of > 0.20 are considered acceptable (Kline, 2005)).

6.4.3 Variance Inflation Factor

The Variance inflation factor (VIF) was calculated as 1/ (1 – R^2). The VIF represents the ratio of total standardised variance to unique variance. Values over 10 are considered to be redundant, although values of 5 or less can be considered to be acceptable for analysis purposes (Sheather, 2009).

6.4.4 Item Loadings

CFA was used to test the relationships between the recorded measures, or indicators, and the latent variables, or factors (Brown and Moore, 2012). Where observed measures are correlated this is because they share a common cause, which is the latent construct. The latent construct accounts for the inter-correlation of the measures by way of a linear function that describes one unique factor and one or more common factors.

The factors were tested to confirm that they were supported by high item loadings to the construct and checked to ensure there was no cross loading of items to multiple factors. Items with standardised loadings of greater than 0.50 were considered significant for the purposes of analysis (Hair et al., 2010).

6.4.5 Factor Correlation

The correlations between factors were calculated and assessed. The recommended 0.85 correlation threshold (Kline, 2005) was used as the benchmark for correlations between factors, ensuring that they showed sufficient discriminant validity.

6.4.6 Composite Reliability (CR)

Calculation of the internal reliability of the constructs using the Cronbach's alpha measure was strengthened by utilising the factor analysis loadings obtained from the CFA analysis to calculate each constructs' composite reliability (Raykov, 1997). The composite reliability takes into account the fact that the items are congeneric, and provides a measure of the reliability of the composed latent variable. In contrast, the Cronbach's alpha value is based on measurements of individual items where each item is assumed to load equally to the factor. Further, CFA also allows for heterogeneous correlations between the indicators and their underlying common factor, allowing a composite reliability score to be calculated with more precision than the alpha scores (Geldhof et al., 2014). The measurement threshold for composite reliability threshold used for composite reliability measurements was 0.7, the same threshold that was used for the Cronbach's alpha.

6.4.7 Average Variance Extracted (AVE)

The AVE represents the amount of variance that is captured by the construct in relation to the amount of variance due to measurement error (Fornell and Larcker, 1981). Calculation of the AVE was made by dividing the sum of the squared factor loadings by the sum squared factor loadings added to the sum of the error variances to produce a measure of the variance extracted from the measurements by application of the factor. Where the AVE is >0.50 the variance due to measurement error is less than the variance extracted due to the construct, lending convergent validity to the model (Bagozzi et al., 1991).

6.4.8 R Square

The R^2 value is obtained by taking the square of the correlation coefficient, and indicates the percentage of the total variance in an independent variable that is explained by the model of which the construct is a part (Hair et al., 2010).

6.4.9 CFA Methods Summary

The techniques outlined in this section were used in confirming the presence and nature of the factors included in the research model. These methods established estimates of item loadings of the measurement indicators on their respective constructs; their correlations and any potential multi-collinearity between the constructs; the amount of unique variance, or measurement error for each indicator;

and the resultant composite reliability and average variance extracted (AVE) attributed to each measurement item in the model.

The results from the CFA process produced a fully characterised measurement model that was central to the SEM modelling process described in the next section.

6.5 SEM Modelling Methods

Structural Equation Modelling (SEM) is a family of statistical modelling techniques that seek to explain the relationships among multiple latent variables that comprise a structural model. They are used to examine the structure of interrelationships expressed in a series of equations, similar to a series of multiple regression equations. SEM models depict all of the relationships among latent constructs (both dependent and independent variables) involved in the analysis. SEM models are used to estimate multiple and interrelated dependence relationships. They also have the ability to represent unobserved concepts in these relationships and account for measurement error in the estimation process (Hair et al., 2010).

SEM is a covariance structure analysis technique and any covariance present between constructs is expressed in a sample covariance matrix. For the purpose of this thesis covariance Based SEM (CB-SEM) was used as the model testing technique. CB-SEM was selected because theory testing, theory confirmation and the comparison of alternative theories was the primary objective of analysis (Hair et al., 2010). Path analysis was used to assess how well the proposed paths matched the structural model, with each of the paths representing a hypothesis to be tested.

6.5.1 Maximum Likelihood Estimation

The modelling process involved using a separate set of relationships for each of a set of dependent variables. SEM estimated a series of separate, but interdependent multiple regression equations simultaneously by specifying the structural model used by the statistical program. The model was constructed to facilitate testing the dependence relationships between the constructs. These relationships were translated into a series of structural equations for each dependent variable, allowing for multiple relationships between dependent and independent variables.

Maximum Likelihood Estimation (MLE) was the statistical method that was utilised to derive parameter estimates. The estimates maximise the likelihood that the data were drawn from the population based on the strength of the covariance between values. Maximum Likelihood is based on the principles of Normal Theory because it assumes that the population distribution of the endogenous variables is multivariate normal, an assumption that rarely holds in research data collection. It has, however, been shown that MLE is robust to deviations of non-normality when the sample size is large (Hu et al., 1992). The method also requires that records have no missing values.

Estimates of parameter values are derived simultaneously using complex fitting functions and the candidate model is fitted iteratively, using start values estimated from the model parameters, and continuing until the improvement in the fitting estimates levels off, leading to a converged solution. The resulting estimated path

coefficients are interpreted as regression coefficients in multiple regression equations. In this way, Maximum Likelihood estimates the coefficients that control for correlations among multiple indicators.

6.5.2 Model Testing Strategy

The strategy utilised in the investigation was the (Anderson and Gerbing, 1988) two-step approach to SEM. SEM models are hierarchical if any model is a subset of another. This allows the modification of models that were iteratively created, tested and sorted for goodness-of-fit (Kline, 2005).

The start point for the approach was by creating and testing a saturated structural sub-model (M_s), where all parameters are freely estimated. The lower bound for the testing strategy was the null model (M_n), were all the parameters that relate the constructs to each other were set to zero, and no relationships were defined. The research model of interest, (M_t) represents the theoretical or substantive model that was fitted iteratively. Structural sub-models of M_t represented the next most likely models with constrained and unconstrained theoretical alternatives (M_c and M_u) such that the five sub-models were nested in a sequence:

$$M_n < M_c < M_t < M_u < M_s$$

The iterative process consisted of a series of iterative sequential Chi Square Difference Tests (SCDTs) that aimed to produce successive fit information for the sub-

models M_t, M_c and M_u and obtain a best sub-model with the lowest chi square statistic within the boundaries of the saturated and null models (M_s and M_n).

This method resulted in the resolution of a model of interest, M_t, that utilised comparisons with the structural constraints from model M_c or the unconstrained alternative M_u , comparing the goodness-of-fit obtained from the SCDTs to determine whether a constraint should be imposed or removed from the test model. Selected weak paths were constrained to zero, generally decreasing the model fit. Adding additional stronger paths decreased the calculated chi square and indicated a better fit. Adding or removing construct measurement observations helped to increase or decrease the number of degrees of freedom, but negatively affected parsimony adjusted fit indexes.

Model testing involves freeing and constraining paths to obtain the best fit to the data. Where paths between constructs not originally specified in the literature were found or altered, targeted literature searches were carried out to ensure that there was a theoretical basis for the observations made. Theoretically based modifications have been shown to be stronger than empirical automatic modifications in ascertaining which models were closer to reality (Silvia and McCallum, 1988). Every path that was included in the model was tested, not only for goodness-of-fit in a statistical sense, but also in correspondence to the prior literature supporting them.

6.5.3 Model Recursion

The research model described a recursive path model. Recursive models have uncorrelated disturbances and all correlation effects are unidirectional. Non-recursive models may have feedback loops or may have correlated disturbances. These disturbances represent the all sources of residual variation in indicator scores that are not accounted for by the constructs (Kline, 2005). Non-recursive models often contain feedback loops. However, to assess true behavioural feedback the research design would have had to be longitudinal in nature to account for delayed feedback effects.

6.5.4 SEM Modelling Methods Summary

Covariance based SEM was used as the method by which to determine the presence of covariance relationships between the models' constructs. The strength of these relationships were calculated using the maximum likelihood method of parameter estimation. A model testing strategy using Anderson and Gerbing's (1988) methodology, resulting in a fitted recursive model from which the research hypotheses could be tested.

The following sections include the fit indexes used in determining the goodness-of-fit, and includes other statistical techniques that were deemed to be of use in the evaluation of the research model.

6.6 SEM Model Fitting

A model is said to fit the observed data to the extent that the model-implied covariance matrix is equivalent to the empirical covariance matrix (Schermelleh-Engel et al., 2003), and the model fit determines the degree to which the structural model matches the sample data.

The general method followed for goodness-of-fit ensures that the model was identified; that the iterative estimation procedure converged; that all parameter estimates were within the range of permissible values; and that the standard errors of the parameter estimates have reasonable size (Marsh and Grayson, 1995). Once a model has been specified and the empirical covariance matrix is given, a method has to be selected for parameter estimation based on the data distribution (Schermelleh-Engel et al., 2003; Bollen, 1990). Parameter estimation using maximum likelihood estimation (MLE) was selected as the method to determine the covariance between the structural elements of the model.

Following successful iterative convergence of the parameter estimation process, a number of fit indexes were used with which to assess how well the proposed model fits the dataset provided. Given the number of different fit indexes available to the researcher (Kline, 2005) recommends the following fit indexes, Chi-Square, RMSEA and the 90% confidence levels, Bentler CFI, SRMR.

6.6.1 Chi Squared Indexes

Chi-squared indexes are a class of indicators of model fit that measure the discrepancies that exist between a model and the data. The model Chi-squared (χ^2_m) is the most widely reported measure of goodness-of-fit (Kline, 2005). A perfectly fitted model will have $\chi^2_m=0$, with higher values indicating a progressively worse fit. As such, χ^2_m actually represents a 'badness of fit' index where higher values indicate less correspondence to the data (Kline, 2005). The null hypothesis has a chi square of zero, so model fit is based on the acceptance of a value that is as close as possible to zero as an indicator of goodness-of-fit. The chi-square fit index assumes that the data displays multivariate normality and model fit is sensitive to the effects of data non-normality, with severely non-normal values giving high values.

Fit indexes such as χ^2_m measure overall error and are therefore sample based indexes. Chi-squared is very sensitive, and increases as a result of the sample size, with larger samples having a higher value (Hair et al., 2010). To compensate for sample size, the chi squared is divided by the number of degrees of freedom (*df*) to produce the normed chi-square χ^2_m/df (NC). The number of degrees of freedom is not a sample based index, it is calculated based on the size of the covariance matrix, which comes from the number of indicators in the model. Each degree of freedom represents a potential axis along which the model can be rejected (Raykov and Marcoulides, 1999). Bollen (1990) notes that values of the NC of up to 5.0 can be indicative of an adequate model fit.

As chi-square is a 'badness of fit' indicator, the probability of the null hypothesis being true must be a close to zero as possible to indicate that it does not hold. Acceptable probability (p) values of <0.05 are recommended to indicate rejection of the null hypothesis. Although there are many reasons why the χ^2_m statistic may not effectively capture the fit of a model to a dataset, a major reason to report the chi-squared is that it is the only inferential fit index, and only for χ^2_m can the researcher make statements about significance and hypothesis testing, with all other fit indexes representing descriptive measures of goodness-of-fit (Iacobucci, 2010).

6.6.2 Other Fit Indexes

The assessment and selection of the goodness-of-fit of the research model was based on the evaluation of a number of fit indexes. The calculation of different fit indexes provides a method with which to compare the model in question with an alternative baseline interpretation of the data. Using fit indexes of different classes help to overcome the shortcomings of relying on a single fit indicator (Jaccard and Wan, 1996).

Incremental fit indexes assess the relative improvement in fit displayed by a model with a baseline model, usually referred to as the independence model. The independence (or null) model assumes that there are zero population co-variances amongst the observed variables. Due to the assumption of unrelated variables, the independence model typically shows much higher chi-squared model values than the

research model, and lower values demonstrate that the research model shows improvement on the baseline model.

- The Comparative Fit index (CFI) relies on how well the non-centrality of the model fits to that of the null hypothesis (Bentler, 1990) and is calculated as the ratio of the non-centrality parameter (Θ) of the research model divided by that of the baseline model expressed as 1- (Θ_m /Θ_b). Values of 0.90 or greater may indicate reasonably good fit to the data (Hu and Bentler, 1999)
- The Normed Fit Index (NFI) compares the model chi-squared to a baseline chi-squared (1- χ^2_m/ χ^2_b). An acceptable fit index for a good model is where the Normed Fit Index (NFI) exceeds 0.90 (Byrne, 2016).
- The Relative Fit Index (RFI) (Bollen, 1989) is also derived from the NFI and includes a model penalty for model complexity by using the degrees of freedom in the model. The TLI (NNFI) is thought to be more useful in interpreting fit than the RFI in most circumstances (Marsh et al., 1996).
- The Incremental Fit Index (IFI) (Bollen, 1989) further adjusts the Normed Fit Index for sample size and degrees of freedom.
- The Tucker Lewis Index (TLI) or Non Normed Fit Index is similar to the NFI but compares the normed chi-squared of the actual and baseline models (1-NC_m/NC_b) (Tucker and Lewis, 1973). In doing so, it penalises for adding additional model parameters, and allows for parsimony of fit.

The choice and comparison of fit indicator is an area where a research report must avoid the partial or incomplete reporting of SEM statistics and assumptions

which can mislead readers and reviewers (Gefen et al., 2011). Authoritative simulation data provided by Hu and Bentler (1999) that a rule of thumb for the IFI and other incremental indexes, including CFI, NFI and TLI is that values greater than 0.9 may indicate reasonably good model fit (Bentler and Chou, 1987).

6.6.3 Root Mean Square Error of Approximation

The RMSEA is a parsimony adjusted index that corrects for model complexity, thus favouring the simplest model when two models with similar explanatory power are being compared. It calculates a non-centrality parameter of the chi-square distribution using the equation:

$$\sqrt{(\chi^2 - df)} / \sqrt{([df - (N-1)])}$$

The non-centrality parameter is used compare the model with a perfect null hypothesis, thus reflecting that modelling involves a degree of approximation rather than exact replication of reality. Like the Chi-square measure on which it is based, RMSEA estimates discrepancy of fit, but does so as the discrepancy per degree of freedom. A value of zero is the best possible model fit, with values of the RMSEA <= 0.05 indicates close approximate fit, and a value between 0.05 and 0.08 suggests a reasonable error of approximation, and values >0.1 representing models with a poor quality of fit (Browne and Cudeck, 1993). An associated indicator, the *p*close, measures how closely fitting the model is, with values less than 0.05 generally accepted as being the cut-off for close fitting models (Hair et al., 2010).

The inclusion of 90% confidence intervals in reporting the RMSEA statistics provide the degree of uncertainty of the 90% level of statistical confidence, taking into account the estimated non-centrality parameter. These intervals also take into account the effects of statistics being subject to population sample error and allow upper and lower bound fit estimates based on the degree of non-centrality.

6.6.4 Standardised Root Mean Square Residual

The goodness-of-fit was assessed using residuals (the difference between the observed and estimated covariance matrices). Residuals reflect the errors in predicting individual observations, but as SEM does not focus on individual observations it represents the difference between the observed and estimated covariance between any pair of indicators.

The Standardized Root Mean Square Residual (SRMR) was calculated by the square root of the difference between the residuals of the sample covariance matrix and the co-variances displayed by the hypothesized model. A high value of SRMR indicates that residuals are large on average, relative to what one might expect from a well-fitting model (Gefen et al., 2011). A good fitting model should have an SRMR value of <0.05 (Hu and Bentler, 1998, 1999). An SRMR value of >0.1 suggests that the model does not explain the corresponding observed correlation very well. (Kline, 2005).

6.6.5 Akaike Information Criterion (AIC)

The AIC belongs to a class of statistics relating to predictive fit indexes that assess the model fit relative to hypothetical replication samples of the same size and randomly drawn from the same population as those of the researchers' sample. AIC is a population based index based on a combination of estimation and selection under a single conceptual model (Lucacs et al., 2007).

The AIC increases or decreases the model chi squared by the number of free model parameters or the number of degrees of freedom, and so favours more parsimonious models when two equivalent models are compared. The model with the lowest AIC is favoured as being the one most likely to replicate.

6.6.6 SEM Model Fitting Summary

This section described the derivation of indexes that were calculated to provide an indication of the average or overall fit of the model to the observed data. As aggregate measures of goodness-of-fit they may give overall good values even when portions of the model have a poor fit. Achieving a good fit does not necessarily reflect that the model makes theoretical sense, and does not guarantee that the model is correct.

The judicious use of indexes provide calculated numbers that summarize the fit and guide the reasoning behind selecting the most appropriate interpretation of the co-variances present. The iterative model trimming strategy employed for testing

ensured that the best possible fit of RMSEA, Fit indexes, and minimum Chi squared results were obtained. These were used as a primary measure of fit that was used in conjunction with sample based indexes, parsimony based indexes, information theory indexes and insights from previous theoretical work to ensure the optimum model fit.

6.7 Model Stability Methods

Establishing model stability across the three scenarios (Retail, Banking and Healthcare secondary use) required that the different scenario measurement models under which the research was carried out yielded equivalent representations of the same constructs (Hair et al., 2010).

6.7.1 Measurement Invariance

The measurement invariance across the three scenarios (Retail, Banking, and Healthcare) was analysed using the method of multi-group confirmatory factors analysis (MGFA) using AMOS. This is a process of comparing measurement models empirically, whilst imposing increasingly restrictive constraints. The fundamental measure of difference for comparison is the Chi-square difference ($\Delta\chi^2$). If the constraints are applied and the model fit does not show a significant increase (worse fit), then the constraints can be accepted.

A six stage modelling process for measuring invariance assesses the model through a series of successive constraints, in terms of the configural invariance (establishing the same basic factor structure for all groups); the metric invariance

(comparison of the equivalence of factor loadings / weights); the measurement intercept invariance (testing the equality of the measured variable intercept values);the structural covariance invariance (constructs are constrained to ensure that they are related to each other in a similar fashion across groups); and the measurement residual invariance (assessment of the equality of variance of residuals not accounted for by factors).

Achieving full invariance becomes increasingly difficult to achieve as the tests progress to the later stages, and a consensus view (Hair et al., 2010) is taken that if tests of configural and metric invariance are met then the partial invariance of the basic structure can be proved and the testing can proceed to the next stage.

6.7.2 Context Models

Predicated on an acceptable measurement invariance across contexts the model fitting process was reapplied to context specific responses using the original model fitted with all observations. This second round of model fitting did not seek to change the structural model or the relationships contained within, but were re-run on a scenario-by-scenario basis to ascertain if the model characteristics were persistent across the contexts.

6.7.3 Model Stability Summary

The applicability of the research model across scenarios was dependent upon determining the presence of an acceptable level of measurement invariance, using the

MCFA methods described in this section. Subsequent re-fitting of the research model to the scenario data subsets was used to re-assess the applicability of the full observation model to these domains.

6.8 Mediation and Moderation

After model fitting and stability testing was complete the techniques of mediation and moderation testing were utilised to explore the mechanisms of how, why and when the cybersecurity variables exerted their influence on trust. Mediation analysis was applied to the full research model to gain insight into how and why independent variables exert influence on the dependent variables, and moderation analysis was used to shed light onto when those effects are likely to be triggered

6.8.1 Path Analysis

Path analysis is a general term for the use of bivariate analysis and correlation to estimate relationships in an SEM model. It was used in the research to determine the strength of the paths depicted in the research path diagram. The measurement model estimated the strength with which the items loaded to the constructs. The structural model was used to assess the level of covariance between the constructs, and the directionality of the relationship between them. This analysis of the paths and their directionality allowed the correlation coefficients to be calculated between the construct diagram nodes, allowing the relationships, and their corresponding hypotheses to be tested.

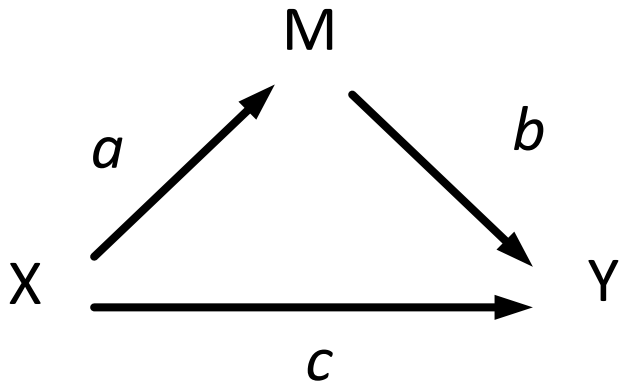
Path analysis research methods were used in the assessment of mediating and moderating variables. These specialised cases of path analysis are described in the following sections.

6.8.2 Mediation Analysis

The analysis of mediating variables in the path model seeks to gain a more accurate explanation of the effect that an independent variable has on a dependent variable. Mediation occurs when a third variable or construct intervenes between two related constructs, and the presence of a mediating process or variable helps to explain the reason why an effect occurs (Hair et al., 2010).

For mediation to happen the independent variable (X) must affect the mediator (M) (path a); secondly, the independent variable(X) must affect the dependent variable (Y) (path c); and thirdly, the mediator (M) must affect the dependent variable (Y) (path b).Figure 6-1 (Baron and Kenny, 1986).

Figure 6-1 Causal Steps Model of Mediation



The effect strength (None, Partial, or Full) of the mediating variable or process was determined by using path analysis of the validated research model with and without the presence of mediating variables. The results were used to interpret the effect strength from the weight and significance of the covariance between the independent and dependent variables. Where significant covariance was detected without the mediator and this was not significant with the mediator then full mediation was inferred. Conversely where a significant covariance was evidenced without the mediator that subsequently became insignificant with the mediating variable then the absence of mediation effects were recorded. The presence of partial mediation was inferred where significant covariance without the mediator was reduced when the mediating variable was added, albeit with a reduced significant effect.

Baron and Kenny's tests (1986) assume normality of the variables under investigation (Normal Theory) of the variables. Further analysis using asymmetry correcting methodology (Mallinckrodt et al., 2006; MacKinnon et al., 2004; Shrout and Bolger, 2002) was performed to ensure that the implied mediation effects seen using the Baron and Kenny and Sobel methods were congruent with the results that took into account statistical asymmetry due to variable skewness and kurtosis.

The software package (AMOS version 25.0.0) was configured to use bootstrapping methods to generate a dataset of 2000 bootstrapped samples from the original dataset (*n*=405) that mirrored the distribution of the collected data. The 95% upper and lower confidence bias corrected intervals for the standardised direct and

indirect effects and the two-tailed significance of the results were recorded. The technique followed the Preacher and Hayes (2004; 2008) recommended procedure for mediation testing.

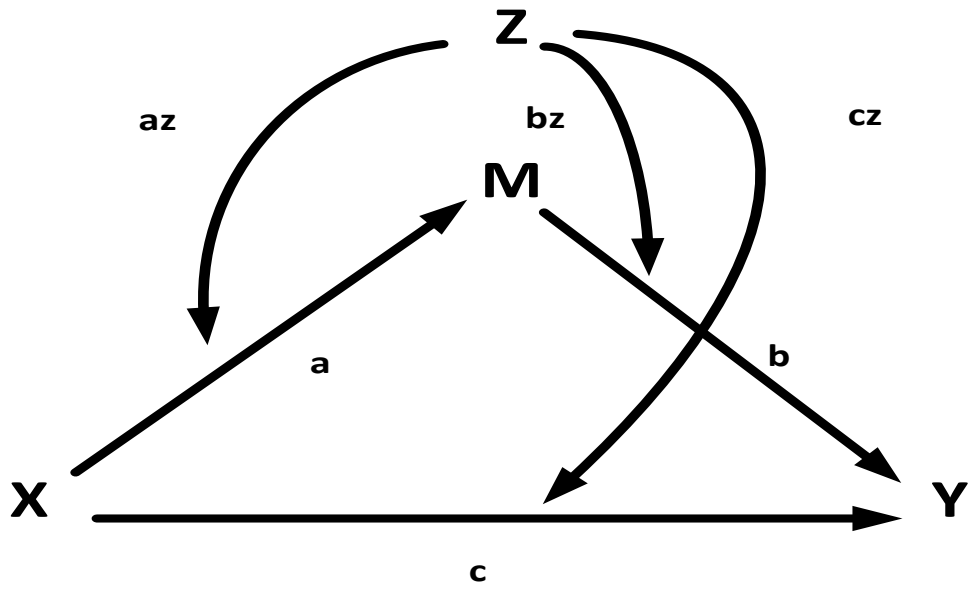
6.8.3 Moderation Analysis

Moderated path analysis is used to assess when the effects of an independent variable on a dependent variable varies with the level of a third variable, (Z) (Baron and Kenny, 1986). The moderator variable regulates the strength of a relationship, and is typically introduced into a model where an inconsistent relation exists between the predictor and criterion variable (Baron and Kenny, 1986). Established procedures for assessing moderation and mediation include the piecemeal approach of combining the causal steps approach with ANOVA based moderation analysis; subgroups analysis of the moderator variable; and a moderated causal steps approach where the causal steps model is augmented with regression terms that evaluate the effect of the moderator variable. However, there are drawbacks to all of these methods (Edwards and Lambert, 2007).

An approach that integrates each of these methods, whilst minimising the drawbacks allowed the direct, indirect and total effects of the moderator variable to be assessed within a framework of mediated moderation (Edwards and Lambert, 2007). Figure 6-2 shows the potential effects that the introduction of a moderator variable can have on mediated paths as part of a total effect moderation model. In the Total Effect Moderation Model the moderation of the first and second stages of the

indirect mediation is combined with moderation of the direct effect. The total effect is calculated by combining the indirect and direct effects. The moderating effect of Z on the relationship X and Y depends upon the level of Z, which can act on both the indirect and direct paths between X and Y.

Figure 6-2 Total Effects Moderation Model



To utilise the method the all of the relevant variables in the relationship were mean centred to allow comparison. Product variables were created to assess the combined influence of the moderator on the independent variable and the mediator variable. SPSS was used to perform OLS regression modelling on the paths, and to estimate the contribution of each of the variables. The paths were evaluated independently of each other. The first stage of testing used M as dependent, with X and Z, and the product XZ as regressors to ascertain the relative weights of the

variables in path a. The second round of regression was used to evaluate path b, using X, M, Z and the product variables XZ and MZ as the regressors.

The estimates of significance were calculated from the SPSS regression procedure output. Additional confidence intervals of 90 and 95% were obtained from the SPSS constrained nonlinear regression (CNLR) procedure using 1,000 bootstrap samples generated using the Stine (1989) method. This provided additional bias corrected confidence intervals for the analysis, necessary due to the use of product variable values that are more sensitive to the effects of non-normal data.

6.8.4 Mediation and Moderation Summary

The technique of path analysis was applied to mediation analysis to provide further insight into how and why the observed effects were produced. These were produced using both Normal Theory methods and asymmetry corrected methods to add detail to the nature of mediation effects. Moderation of the key mediated relationships were undertaken using the Edwards and Lambert (2007) methodology to provide further clarity as to when moderating effects would take place.

6.9 Research Methods Chapter Conclusion

The methods detailed in this chapter were chosen to maximise the validity of the measures and measurement model, the constructs built on the measurement model and the structural model built on the constructs. The research methods ensured that the analysis performed was part of a verifiable chain of data custody that

ensured the reliability and validity of the analysis and purified and reduced the estimated error conditions based on the scaled questionnaire responses that were collected for analysis.

The following chapter, **Chapter 7, Descriptive data Analysis** details the univariate analysis results calculated using the research method techniques outlined in this chapter.

7. Descriptive Data Analysis

The descriptive statistical methods outlined in the previous chapter, **Chapter 6, Research Methods** were calculated using the scaled, formatted and face valid data set obtained as a result of the data collection process. Descriptive analysis was used to ascertain the univariate normality, distribution and suitability of the collected values.

7.1 Introduction

The descriptive data process was implemented because the multivariate data analysis techniques in this thesis rely heavily on the assumption of normality or near-normality of the component values which is often difficult to justify in practice (Liu et al., 1999). The prior assessment of the normality of the input values lends weight to the assumption that the results of the multivariate analysis were not unduly affected or biased by the presence of non-normal data. Severely non-normal data has an impact on Maximum likelihood Estimation (MLE) usage (Cousineau et al., 2004), and can reduce the validity of bootstrapping methods used in multivariate analysis methods (Bollen, 1989). Confirming the univariate normality of observations reduces the possibility of a Type I error (by rejecting the null hypothesis when it should be accepted) or a Type II error (that of failing to reject the null hypothesis when it should be rejected).

The calculation of the means and distribution of the data reduced the probability of these types of errors by ensuring that the calculations were based on robust data that were assessed for non-normal indicators before they were utilised for hypothesis testing purposes.

7.2 Survey Characteristics

Preliminary analysis of the data set was performed to ensure that the whole set characteristics of the collected data were suitable for univariate analysis purposes. This took the form of assessing the number of fully completed survey responses to provide prima facie evidence that the sample met the prior requirements for testing and analysis purposes.

7.2.1 Sample Size

The actual number of questionnaires completed and cleansed (n=405) counted as a large sample. The larger sample size is recommended to aid more complex modelling (Kline, 2005) and to provide a more stable solution (Hair et al., 2010). It can be shown that larger sample sizes reduce the detrimental effects of non-normality by reducing the aggregate effects of outliers.

7.2.2 Survey Scenarios

The completed questionnaires for the scenarios (Table 7.1 Sample Sizes) also provided adequate, comparatively sized sample observations to utilise Structural

Equation Modelling analysis techniques (Retail scenario n=133, Banking scenario n=136, Healthcare scenario n=136).

Table 7.1 Sample Sizes

Scenario	Number of Respondents (n)	Valid Percent	Cumulative Percent
Retail	133	32.8	32.8
Banking	136	33.6	66.4
Healthcare	136	33.6	100.0
Total	**405**	**100.0**	

7.2.3 Missing Data

The data collection was comprised of fully completed questionnaire responses only, with no partial or unfilled fields being utilised. This was strengthened by the electronic means of data collection whereby each question had a non-optional response required. However, it was noted that five survey responses (1.2%) were missing demographic data responses. These were removed via list wise deletion of the relevant records, with the number of remaining fully filled in survey responses as *n*=405.

The use of fully filled in questionnaires ensured that the data collected were directly from the respondents, and precluded the need to synthesise, replace or substitute values by the researcher. The wider implications of missing data and of providing or synthesising missing information to calculate parameter estimates using Maximum Likelihood techniques (Enders and Bandalos, 2001) were also avoided by adding this regulation to the data collection phase.

7.2.4 Survey Characteristics Summary

This section detailed the statistics relevant to the overall survey observations collected. The sample size and scenario responses, after cleansing and data inspection was of sufficient number (*n*=405) and quality to proceed both with the techniques of univariate normality analysis, but also to provide a data set without missing data with which multivariate data analysis techniques could also be used.

7.3 Demographics

As part of the data collection exercise, simple, anonymous demographic data was captured from the survey respondents. Demographic data operates across the survey, and represents persistent data on characteristics that is independent of the survey environment or the scenario tested. The areas of demographic data include those relating to the self-reported personal characteristics of the respondent (Gender, Age Group and Education Level)

Where the responses were captured in ordinal scales, one-sample Chi-squared tests of normality were performed to ensure that the groups were not significantly different from the expected distribution, and therefore suitable for analysis.

7.3.1 Gender

The respondent population sample was comprised of 219 females and 186 males (Table 7.2). Binary classification of the data meant that further statistical data descriptions were not required.

Table 7.2 Respondent Gender and Scenario

	Gender		
	Male	**Female**	**Total**
Retail	64	69	133
Banking	61	75	136
Healthcare	61	75	136
Total (n)	186	219	405

7.3.2 Age Group

The survey participants were asked to self-report their age group (Table 7.3). The mode was in the 55-64 age category. A chi-squared test was run on the data to see if participant ages could be classed as being significantly different. This yielded χ^2= 98.748, *df* =5, p<0.001 indicating that the variance from a hypothesised expected distribution was not significant, and could be accepted for analysis purposes.

Table 7.3 Respondent Age Group

Age Group	Frequency	Percent	Cumulative Percent	UK Estimate Percent*
Under 25	16	4.0	4.0	6.4
25-34	35	8.6	12.6	13.5
35-44	59	14.6	27.2	12.7
45-54	96	23.7	50.9	13.9
55-64	103	25.4	76.3	11.7
Over 65	96	23.7	100.0	15.7
Total	**405**	**100.0**		

* Source UK ONS mid-year population estimates (ONS, 2017). Under 25 represents the population proportion aged 20-24 as participants were required to be over 18. Over 65 age group represents UK residents aged 65-84.

The sample was further subdivided to show the number and age group of respondents that completed the different scenarios (Table 7.4)

Table 7.4 Scenario by Age Group

	Scenario Retail	Banking	Healthcare	Total
Under 25	7	1	8	16
25-34	10	14	11	35
35-44	20	17	22	59
45-54	28	31	37	96
55-64	36	36	31	103
Over 65	32	37	27	96
Total (n)	**133**	**136**	**136**	**405**

7.3.3 Education Level

Participants were also asked to report their level of education as part of the preliminary demographic questions (Table 7.5). The modal value of this categorical variable was that of 'Finished School'. All education levels were represented in the survey.

Table 7.5 Respondent Education Level

Education Level	**Frequency**	**Percent**	**Cumulative Percent**
None	5	1.2	1.2
Some Schooling	8	2.0	3.2
Finished School	146	36.0	39.3
College Study, not degree level	110	27.2	66.4
Degree Level	99	24.4	90.9
Postgraduate Level	37	9.1	100.0
Total	**405**	**100.0**	

The one sample chi-square test produced values of χ^2= 256.852, d*f* =5, p<0.001, confirming that the spread of values was not significantly different from the hypothesised expected values.

7.3.4 Demographics Summary

As a preliminary part of the online survey, simple demographic data about gender, age group and education level were sought from the respondents. This data was found not to be significantly different to that expected, and all categories of data were represented in the survey. The percentages of respondents were benchmarked with the official ONS 2017 population estimates (ONS, 2017) that suggested that the respondents were over-represented in the 45-64 age group relative to the UK population average.

Respondents also filled in a series of questions that related to their attitudes towards digital interaction, and these responses are analysed in the next sub section.

7.4 Respondent Attitudes

Survey respondents answered a short series of questions relating to their attitude to transactions online (their online risk attitude), their self-reported levels of awareness of threats posed by online environments (cybersecurity awareness), and their opinion of their sensitivity to privacy disclosure (their privacy sensitivity).

7.4.1 Online Risk Attitude

The respondents were required to answer a question on their attitude to engagement with digital environments. The items were taken from (Myers et al., 2003) as a proxy for the respondents trusting attitude translated to the digital medium. The responses are detailed in (Table 7.6).

Table 7.6 Trusting Preferences Online

Preference	Frequency	Valid Percent	Cumulative Percent
Trusting others with whom I have experience.	161	39.8	39.8
I rely more on possibilities and risk taking in online environments.	52	12.8	52.6
I analyse situations logically and objectively before acting.	192	47.4	100.0
Total	**405**	**100**	

The data revealed that similar percentages of respondents reported that their interactions online were governed by trust or logical analysis, with only 12.8% of respondents being reliant on utilising the medium to explore possibilities or acknowledging and taking risk. The finding that only a small percentage of respondents considered themselves to be online risk takers resulted in the withdrawal from the model of the construct named 'Safety' which also displayed low item loadings from subsequent CFA analysis as it was deemed to be a low priority concern for the majority of users.

7.4.2 Cybersecurity Awareness Levels

Respondents were asked to give a response to the question *"How much have you heard or read during the last year about the use and potential misuse of the information collected from the Internet?"* The recorded responses were coded as being a measure of how aware of the cybersecurity environment the respondents were (Table 7.7). The coded responses displayed a symmetry around the mean value of 'a moderate amount', and the data described a near normal distribution of 1.06. The lack of variance in responses was confirmed by the chi-square test with χ^2= 125.259, d*f* = 4, p<0.001.

Table 7.7 Cybersecurity Awareness

Cybersecurity Awareness			
Response	**Frequency**	**Valid Percent**	**Cumulative Percent**
A great deal	27	6.7	6.7
A lot	101	24.9	31.6
A moderate amount	152	37.5	69.1
A little	86	21.2	90.4
None at all	39	9.6	100.0
Total	**405**	**100.0**	

7.4.3 Privacy Sensitivity Levels

Survey respondents were also required to answer the question "C*ompared to others, I am more sensitive about the way online companies handle my personal information"*. The responses to this question were coded as being indicative of the individual privacy sensitivity (Table 7.8). The mean value was between neither

agreeing nor disagreeing about sensitivity; and agreeing that they are sensitive about their privacy online, displaying a slight skewness towards agreeing they were sensitive. The chi-square test indicated that the distribution did not differ significantly from the expected value with $\chi^2 = 269.497$, d$f = 4$, $p<0.001$.

Table 7.8 Privacy Sensitivity

Value	Frequency	Valid Percent	Cumulative Percent
Strongly disagree	3	0.7	0.7
Disagree	47	11.6	12.3
Neither agree nor disagree	182	44.9	57.3
Agree	133	32.8	90.1
Agree strongly	40	9.9	100.0
Total	**405**	**100.0**	

7.4.4 Respondent Attitudes Summary

The additional attitude background questions related to the respondents' attitude towards trust online, their level of cyber security awareness, and their self-reported privacy sensitivity. The responses were found not to be significantly different to those that were expected. As a result of the descriptive statistics analysis of the demographic and attitude responses the co-variant data were found to be suitable for use in analysis.

7.5 Model Construct Normality

Multivariate analysis requires that the assumptions underlying statistical techniques be tested twice: first for the separate variables, and secondly for the multivariate model variate (Hair et al., 2010). Multivariate normality involves the

generalisation of the univariate normal distribution to the case of *p* variables, and normality is an assumption that underlies the validity of significance tests in MANOVA.

To this end, the constructs utilised in establishing the significance of the hypotheses, and which were composed of separate measurement items, were subject to normality assessment. The SEM structural model expressed the covariance between constructs. These constructs were created as aggregated measures of the component measurement items that constituted them in the measurement model. Reporting the underlying univariate and multivariate normality statistics for the constructs is based on the finalised constructs following item purification using reliability assessment, multi-collinearity detection and factor loadings.

7.5.1 Item Coding

There were initially 45 items in the survey questionnaire. As a result of analysis utilising EFA and CFA techniques this number was reduced to 19 items that displayed the strongest loadings to the constructs utilised in the research model. These items are listed in Table 7.9 along with the ID used to identify the items in the sections that follow.

The items were anchored to the salient attributes of the construct detailed in Table 5.1. Anchoring items to attributes allowed the scope of the constructs to be defined precisely.

Table 7.9 Item Coding

ID	Item	Anchoring
CQ1	Any notifications I receive from the organisation are relevant and timely.	Message Relevance
CQ2	The organisation will deal calmly and efficiently with any unexpected events.	Calm
CQ3	Interaction with the organisation is generally constructive and supportive.	Support
DE1	I trust the organisation enough to allow it to delegate the task of fulfilling my instructions to another person or information system.	Action
DE2	I believe that if the organisation delegated tasks it was to help achieve my goals.	Goal attainment
DE3	I can trust the organisation or their agent to act in my place.	Acting in place of trustee
OC1	Allowing the organisation to update records electronically /achieve the transaction gave me the confidence to engage with the same provider again.	Post Hoc evaluation
OC2	I am able to give objective feedback to the organisation or the service provider.	Feedback
SE1	The organisation appears to value the importance of security.	Congruence with customer
SE2	Information security is a key normal behaviour of the organisation.	Information handling norms
TR1	The organisation would not knowingly do anything to harm me.	Confidence
TR2	I know that my information is safe and access is limited only to authorised personnel.	'knowing'
TR3	I believe that the information privacy assurances offered by the organisation will be honoured.	Belief
RE1	The organisation has a reputation for being honest.	Honesty
RE2	Sound principles seem to guide the behaviour of the organisation.	Principled
RE3	The organisation has a reputation for looking after its patients/customers.	Care

7.5.2 Communication Quality

The descriptive statistics for the communication quality construct (Table 7.10) were calculated and showed that the mean values that were in the range 3.93 to 3.95,

displaying almost equal influence on the resultant construct. The data were negatively skewed and displayed a variable amount of kurtosis in the range -.215 to .536.

Table 7.10 Communication Quality Descriptive Statistics

Communication Quality								
ID	**Item**	**Min**	**Max**	**Mean**	**SD**	**Variance**	**Skewness**	**Kurtosis**
CQ1	Any notifications I receive from the organisation are relevant and timely.	1	5	3.93	.891	.794	-.492	-.215
CQ2	The organisation will deal calmly and efficiently with any unexpected events.	1	5	3.95	.877	.770	-.567	.289
CQ3	Interaction with the organisation is generally constructive and supportive.	1	5	3.95	.869	.755	-.655	.536
CQ	**Composite Construct – Communication Quality**	**1**	**5**	**3.94**	**.767**	**.588**	**-.490**	**.226**

7.5.3 Delegation

The measures of normality applied to the delegation construct are detailed in Table 7.11. Item DE2 was the most influential and DE3 was least influential indicator based on mean values. The values were negatively skewed and slightly leptokurtic but not considered to be severely non-normal for the purposes of analysis.

Table 7.11 Delegation Descriptive Statistics

Delegation								
ID	**Item**	**Min**	**Max**	**Mean**	**SD**	**Variance**	**Skewness**	**Kurtosis**
DE1	I trust the organisation enough to allow it to delegate the task of fulfilling my instructions to another person or information system.	1	5	3.68	.977	.954	-.533	.019
DE2	I believe that if the organisation delegated tasks it was to help achieve my goals.	1	5	3.75	.900	.810	-.537	.435
DE3	I can trust the organisation or their agent to act in my place.	1	5	3.65	.899	.807	-.403	.263
DE	**Composite Construct – Task Delegation**	**1**	**5**	**3.70**	**.781**	**.611**	**-.444**	**.658**

7.5.4 Outcomes

The statistics calculated for the two-item construct outcomes are detailed in Table 7.12. The measurement variables for the construct displayed similar mean values, indicating they were equal contributors to the construct mean score. The data were slightly negatively skewed and showed variable amounts of kurtosis. The variance and standard deviation described a distribution that was not closely normal, but were not considered to be acute for the purposes of data analysis.

Table 7.12 Outcomes Descriptive Statistics

Outcomes								
ID	**Item**	**Min**	**Max**	**Mean**	**SD**	**Variance**	**Skewness**	**Kurtosis**
OC1	Allowing the organisation to update records electronically /achieve the transaction gave me the confidence to engage with the same provider again.	1	5	3.86	.825	.681	-.238	-.203
OC2	I am able to give objective feedback to the organisation or the service provider.	1	5	3.80	.895	.801	-.502	.344
OC	**Composite Construct – Outcomes**	**1**	**5**	**3.83**	**.753**	**.568**	**-.252**	**.019**

7.5.5 Security

The security construct (Table 7.13) was comprised of two measurement items that displayed mean values in the range 3.93 to 4.05, with item SE2 being slightly more influential in the value of the construct. The variance and standard deviation values, combined with negative skew and positively peaked kurtosis values described a relatively broad peaked distribution with values concentrated at the upper range of the scale and thin tails. None of the values calculated indicated extreme values for the purposes of multivariate analysis purposes.

Table 7.13 Security Descriptive Statistics

Security								
ID	**Item**	**Min**	**Max**	**Mean**	**SD**	**Variance**	**Skewness**	**Kurtosis**
SE1	The organisation appears to value the importance of security.	1	5	3.93	.861	.741	-.644	.262
SE2	Information security is a key normal behaviour of the organisation.	1	5	4.05	.870	.757	-.644	.034
SE	**Composite Construct – Security**	**1.5**	**5**	**3.99**	**.783**	**.614**	**-.526**	**-.149**

7.5.6 Trust

The measurement variables associated with the trust construct (Table 7.14) showed that item TR3 had the most influence on the mean value (3.96), with TR2 (3.76) having less influence on the aggregate score. The values were negatively skewed with a variably platykurtic spread of values. As such, the distribution of the values was non-normal, but not considered to be severe for the purposes of analysis.

Table 7.14 Trust Descriptive Statistics

Trust								
ID	**Item**	**Min**	**Max**	**Mean**	**SD**	**Variance**	**Skewness**	**Kurtosis**
TR1	The organisation would not knowingly do anything to harm me.	1	5	3.92	.965	.931	-.733	.283
TR2	I know that my information is safe and access is limited only to authorised personnel.	1	5	3.76	.889	.790	-.537	.234
TR3	I believe that the information privacy assurances offered by the organisation will be honoured.	1	5	3.96	.879	.773	-.797	.952
TR	**Composite Construct – Trust**	**1**	**5**	**3.80**	**.819**	**.671**	**-.553**	**.424**

7.5.7 Reputation

Reputation (Table 7.15) was measured using measures that displayed mean values between 3.76 and 3.96, with item RE3 being the highest and RE2 being the lowest contributors to the construct mean. At construct level, there was moderate variance and standard deviation from a normal distribution, with the variables displaying some negative skewness and variable but low kurtosis values.

Table 7.15 Reputation Descriptive Statistics

Trustworthiness								
ID	**Item**	**Min**	**Max**	**Mean**	**SD**	**Variance**	**Skewness**	**Kurtosis**
RE1	The organisation has a reputation for being honest.	1	5	3.83	.909	.826	-.486	.039
RE2	Sound principles seem to guide the behaviour of the organisation.	1	5	3.76	.862	.743	-.397	.352
RE3	The organisation has a reputation for looking after its patients/customers	1	5	3.96	.878	.771	-.519	-.033
RE	**Composite Construct-Reputation**	**1**	**5**	**3.85**	**.766**	**.586**	**-.411**	**.196**

7.5.8 Multivariate Normality Assessment

Establishing the multivariate normality of the data used in testing the model is a procedure for which there is no definitive set of tests and methods (Kline, 2005). Testing for multivariate outliers in the dataset was achieved by calculating the Malhanobis distance, a measure of multidimensional distance that assessed all observations to ascertain if any influential outliers were present. No observations of

p>0.5 (Hair et al., 2010) were detected, with the greatest outlier value of 0.19 recorded, indicating good data normality.

In addition, measures of the critical values of multivariate kurtosis and skewness were calculated for all items (Table 7.16). Comparison with the guideline values for the critical ratios (Section 6.2.4) indicated that Kurtosis values were in the low to moderate range, with the skewness values indicating higher, but not severely skewed data.

Table 7.16 Normality Assessment

Variable	Skew	Skewness critical ratio	Kurtosis	Kurtosis critical ratio
CO3	-.653	-5.362	.515	2.115
CO1	-.490	-4.024	-.228	-.935
RE3	-.517	-4.245	-.047	-.195
TR2	-.535	-4.394	.216	.889
TR3	-.794	-6.521	.925	3.800
RE1	-.484	-3.977	.023	.096
OC2	-.500	-4.108	.325	1.336
OC1	-.237	-1.950	-.215	-.885
SE1	-.642	-5.273	.244	1.001
SE2	-.642	-5.273	.018	.076
DE1	-.531	-4.361	.004	.016
DE2	-.535	-4.396	.415	1.704
DE3	-.401	-3.295	.245	1.006
RE2	-.396	-3.250	.333	1.369
CO2	-.565	-4.639	.270	1.110
TR1	-.730	-5.997	.265	1.089
Multivariate			143.790	60.286

7.5.9 Model Construct Summary

The univariate normality of the constructs used statistical techniques to calculate the descriptive terms necessary to describe the normality of the underlying survey response items. Applying the same techniques to the constructs ensured that when considered together they still retained sufficient multidimensional normality to be considered for further analysis purposes.

The assessment of the constructs and their component measures did not detect any outliers in the datasets. The range of all variables reported a full range of values. The mean, standard deviation, variance, and skewness of the constructs typically described negatively skewed distributions at the upper range of the scales (3.70 to 4.36), with narrow variance and standard deviation. Statistical tests of skewness and kurtosis did not exceed the recommended thresholds of (±) 2.58 for skewness and (±) 1.96 for kurtosis (Hair et al., 2010). Kurtosis values were variable but not extreme describing both broad and slender distribution peaks with variable tails. Assessment of the items and calculation of the critical ratios did not find any values that were deemed unsuitable for multivariate analysis.

The analysis did not find any of the constructs possessing a full normal distribution. However, there were also no extreme values reported that could have detrimentally affected the assumption of the near normality of the values obtained.

7.6 Descriptive Analysis

The contribution of this thesis is the production of evidence there are links between information security and trust, and that these links are present and stable across the survey scenarios that were used in the data collection.

To demonstrate the stability of the research findings across the research, it is necessary to assess the significance of the deviations in responses to the questionnaire that have arisen as a result of the demographic make-up of the survey respondents. This is achieved by a comparison of the mean scores attributed by different demographic groups, a one-way ANOVA to assess the F-statistic and p-value significance of the variation between and within demographic groups, and a Levene test of homogeneity of variance that the demographic exerts on the constructs. Analysis of the effects due to the demographic differences in Gender, Age Group and Education Level are included in this section.

7.6.1 Gender Descriptive Analysis

To ensure that any variances in the sample population that were not attributable to the differences in the gender of respondents, the constructs were cross-tabulated with gender to ensure that there were no major differences in the mean and standard deviation for the two samples (Table 7.17). The analysis suggested only small differences between groups.

Table 7.17 Comparison of Means by Gender and Construct

Gender		Communication Quality	Delegation	Outcomes	Information Confidentiality	Security	Trust	Reputation
Male	Mean	3.88	3.65	3.70	4.34	3.92	3.74	3.80
	N	186	186	186	186	186	186	186
	Std. Dev	.793	.813	.716	.655	.809	.856	.795
Female	Mean	4.00	3.74	3.81	4.38	4.05	3.84	3.89
	N	219	219	219	219	219	219	219
	Std. Dev	.742	.753	.628	.633	.757	.785	.739
Total	**Mean**	**3.94**	**3.70**	**3.76**	**4.36**	**3.99**	**3.80**	**3.85**
	Diff	**-0.12**	**-0.09**	**-0.11**	**-0.04**	**-0.07**	**-0.08**	**+0.09**
	N	**405**	**405**	**405**	**405**	**405**	**405**	**405**
	Std. Dev	**.767**	**.781**	**.671**	**.643**	**.783**	**.819**	**.766**

Further analysis of the variance between genders is detailed in Table 7.18 and shows that there is no significant difference between the F-statistic of variance between the groups. To test that the group variances from the mean values observed were distributed evenly across the range of responses the Levene test was carried out to ensure the constructs displayed homoscedasticity. None of the tests revealed significant differences in the homogeneity of the construct variables between gender groups.

Table 7.18 Analysis of Variance (ANOVA) by Gender and Construct

		Sum of Squares	Df	Mean Square	F	F stat Sig.	Levene Statistic	Levene Sig.
Communication Quality	Between Groups	1.377	1	1.377	2.349	.126	.735	.392
	Within Groups	236.316	403	.586				
	Total	237.694	404					
Delegation	Between Groups	.871	1	.871	1.428	.233	.005	.943
	Within Groups	245.793	403	.610				
	Total	246.664	404					
Information Confidentiality	Between Groups	.168	1	.168	.405	.525	.029	.865
	Within Groups	166.824	403	.414				
	Total	166.991	404					
Outcomes	Between Groups	1.235	1	1.235	2.752	.098	1.435	.232
	Within Groups	180.879	403	.449				
	Total	182.114	404					
Security	Between Groups	1.712	1	1.712	2.802	.095	1.992	.159
	Within Groups	246.266	403	.611				
	Total	247.978	404					
Trust	Between Groups	.965	1	.965	1.441	.231	.834	.362
	Within Groups	269.963	403	.670				
	Total	270.929	404					
Reputation	Between Groups	.897	1	.897	1.532	.217	.292	.589
	Within Groups	236.037	403	.586				
	Total	236.934	404					

7.6.2 Age Group Descriptive Analysis

The research constructs and age groups of respondents cross tabulation ascertained whether age group had an influence on the average ratings given for each construct (Table 7.19). It was noted that the older age groups rated most scale items higher than younger participants, with information confidentiality showing a consistent increase with age group.

Table 7.19 Comparison of Means by Age Group and Construct

Age Group		Communication Quality	Delegation	Information Confidentiality	Outcomes	Security	Trust	Reputation
Under 25	Mean	3.33	3.60	3.81	3.52	3.50	3.33	3.31
	N	16	16	16	16	16	16	16
	Std. Dev	1.074	.586	.834	.632	1.032	1.095	.915
25-34	Mean	3.76	3.59	3.80	3.62	3.66	3.67	3.55
	N	35	35	35	35	35	35	35
	Std. Dev	.674	.705	.687	.537	.873	.728	.571
35-44	Mean	3.74	3.65	4.07	3.72	3.89	3.66	3.76
	N	59	59	59	59	59	59	59
	Std. Dev	.695	.736	.646	.699	.713	.723	.755
44-54	Mean	3.99	3.73	4.43	3.81	4.00	3.78	3.88
	N	96	96	96	96	96	96	96
	Std. Dev	.735	.826	.619	.609	.764	.845	.783
55-64	Mean	3.90	3.65	4.48	3.69	3.97	3.70	3.80
	N	103	103	103	103	103	103	103
	Std. Dev	.854	.903	.586	.774	.816	.927	.836
Over 65	Mean	4.24	3.79	4.62	3.90	4.28	4.12	4.12
	N	96	96	96	96	96	96	96
	Std. Dev	.587	.674	.407	.625	.624	.589	.610
Total	**Mean**	**3.94**	**3.70**	**4.36**	**3.76**	**3.99**	**3.80**	**3.85**
	N	**405**	**405**	**405**	**405**	**405**	**405**	**405**
	Std. Dev	**.767**	**.781**	**.643**	**.671**	**.783**	**.819**	**.766**

Analysis of variance (Table 7.20) demonstrated significant variance between age groups for the constructs communication quality, information confidentiality, security, trust and reputation. The variation in responses with reference to these indicator variables was different as a result of the age group demographic.

Table 7.20 Analysis of Variance (ANOVA) by Age Group and Construct

		Sum of Squares	Df	Mean Square	F	F Stat Sig.	Levene Statistic	Levene Sig.
Communication Quality	Between Groups	18.340	5	3.668	6.672	.000	3.395	.005
	Within Groups	219.354	399	.550				
	Total	237.694	404					
Delegation	Between Groups	1.903	5	.381	.621	.684	2.317	.043
	Within Groups	244.761	399	.613				
	Total	246.664	404					
Information Confidentiality	Between Groups	29.022	5	5.804	16.786	.000	6.101	.000
	Within Groups	137.969	399	.346				
	Total	166.991	404					
Outcomes	Between Groups	4.325	5	.865	1.941	.087	1.457	.203
	Within Groups	177.789	399	.446				
	Total	182.114	404					
Security	Between Groups	16.211	5	3.242	5.582	.000	2.795	.017
	Within Groups	231.767	399	.581				
	Total	247.978	404					
Trust	Between Groups	16.239	5	3.248	5.088	.000	4.556	.000
	Within Groups	254.690	399	.638				
	Total	270.929	404					
Reputation	Between Groups	15.459	5	3.092	5.570	.000	3.975	.002
	Within Groups	221.475	399	.555				
	Total	236.934	404					

Additional testing of the effects of age group on the research constructs was undertaken by calculating the Levene test of homogeneity of variance. This demonstrated that all of the constructs, with the exception of outcomes displayed significant heteroscedasticity as a result of being partitioned by age group.

7.6.3 Education Level Descriptive Analysis

The variation in the mean values of the constructs with respect to the respondent level of education is detailed in Table 7.21. This did not reveal any clear-cut correlations between the reported levels of the construct and the education level reported.

Table 7.21 Comparison of Means by Education Level by Construct

Education Level		Communication Quality	Delegation	Outcomes	Security	Trust	Reputation
None	Mean	3.60	3.67	3.27	3.50	3.27	3.33
	N	5	5	5	5	5	5
	Std. Dev	.830	.624	.365	.866	.641	.333
Some Schooling	Mean	4.21	3.96	4.08	4.38	4.42	4.38
	N	8	8	8	8	8	8
	Std. Dev	.616	.825	.868	.791	.427	.547
Finished School	Mean	3.92	3.61	3.72	3.94	3.73	3.81
	N	146	146	146	146	146	146
	Std. Dev	.758	.785	.649	.778	.850	.776
College Study, not degree level	Mean	4.07	3.83	3.90	4.04	3.92	3.96
	N	110	110	110	110	110	110
	Std. Dev	.738	.755	.661	.753	.755	.778
Degree Level	Mean	3.87	3.62	3.72	4.05	3.73	3.77
	N	99	99	99	99	99	99
	Std. Dev	.862	.840	.688	.806	.858	.810
Postgraduate Level	Mean	3.85	3.79	3.58	3.89	3.79	3.82
	N	37	37	37	37	37	37
	Std. Dev	.607	.650	.651	.809	.775	.553
Total	**Mean**	**3.94**	**3.70**	**3.76**	**3.99**	**3.80**	**3.85**
	N	**405**	**405**	**405**	**405**	**405**	**405**
	Std. Dev	**.767**	**.781**	**.671**	**.783**	**.819**	**.766**

Analysis using one-way ANOVA (Table 7.22) revealed significant variance of the means in the constructs information confidentiality and outcomes as a result of comparison with education level.

Table 7.22 Analysis of Variance (ANOVA) by Education Level and Construct

		Sum of Squares	*Df*	Mean Square	F	F Stat Sig.	Levene Statistic	Levene Sig.
Communication Quality	Between Groups	3.721	5	.744	1.269	.276	1.406	.221
	Within Groups	233.973	399	.586				
	Total	237.694	404					
Delegation	Between Groups	4.466	5	.893	1.471	.198	.214	.916
	Within Groups	242.198	399	.607				
	Total	246.664	404					
Information Confidentiality	Between Groups	8.981	5	1.796	4.536	.000	.749	.587
	Within Groups	158.011	399	.396				
	Total	166.991	404					
Outcomes	Between Groups	5.920	5	1.184	2.681	.021	.615	.688
	Within Groups	176.194	399	.442				
	Total	182.114	404					
Security	Between Groups	3.678	5	.736	1.201	.308	.082	.995
	Within Groups	244.300	399	.612				
	Total	247.978	404					
Trust	Between Groups	7.341	5	1.468	2.223	.051	1.521	.182
	Within Groups	263.588	399	.661				
	Total	270.929	404					
Reputation	Between Groups	5.738	5	1.148	1.980	.081	2.309	.044
	Within Groups	231.196	399	.579				
	Total	236.934	404					

Testing for homogeneity of variance between the constructs and the respondent education level revealed there was only homogeneity of variance of statistical significance present in the reputation construct.

7.6.4 Descriptive Analysis Summary

Prior to multidimensional analysis, an initial descriptive analysis of the proposed constructs against the sample demographic groups was performed using SPSS. This was to ascertain whether the measures and constructs displayed sufficiently normal variance characteristics to effectively utilise multivariate statistical techniques on the sample. The methods used for the comparison of the demographics with the constructs were the comparison of mean values, ascertaining the F-statistic and significance of group differences in variance, and calculating the Levene test of homogeneity of variance.

It was found that there was no significant difference in mean and F-statistic of the constructs by respondent gender groups. It did find that the variance detected was not dispersed homogeneously between the groups. Age group comparison of construct means and variance showed a significant difference in the reported values between the groups. The Levene tests demonstrated that the variance of values was present and that it was dispersed evenly throughout the constructs' range. Education levels ANOVA showed that the variance present in information confidentiality and outcomes was significant and that only reputation displayed unevenly distributed variance across the range of education levels.

In conclusion, the use of descriptive statistical analysis revealed that the mean and variance of the constructs were fully stable across the participant gender groups, with some heteroscedasticity in the variance present. Education level displayed mostly

consistent variance and homogeneity. Age group showed greater mean and variance scores and had evenly dispersed variance when compared by age group. This finding militated against the use of gender and education level as reliable predictors of data with normal variance and homoscedasticity when used to interpret the findings of the multivariate data analysis techniques.

7.7 Descriptive Analysis Conclusion

Descriptive statistics serve the purpose of describing the basic features of the data collected as a part of the research. Assessing and checking the data that were collected is an essential part of ensuring that the raw materials used in the production of inferential, multivariate statistics are not compromised or unduly influenced by the presence of poor quality input variables.

The analysis comprised of an assessment of the following areas. The overall survey characteristics; a breakdown of the persistent demographic data items that were collected; evaluation of the attitude based indicators that were subsequently used for moderation analysis; appraisal of the normality characteristics of the constructs used in modelling; and a one-way ANOVA analysis of the effects of the demographic fields on these constructs. These were performed to ensure that the univariate characteristics were fully congruent with the aim of producing well-formed multivariate inferences.

Based on the reasonably normalised distributions revealed by the descriptive analysis the traits of univariate normality were deemed to be suitable to proceed with

the multivariate analysis. Based on these distributions the use of AMOS version 25.0.0 was used to carry out this analysis in preference to tools that do not require normalised data distributions. The analyses fulfilled as part of the research are detailed in the next chapter, **Chapter 8, Multivariate Data Analysis**.

8. Multivariate Data Analysis

The descriptive characteristics of the collected survey response data presented in the previous chapter underpin an essential element of the data evaluation process, by ascertaining that the preparation, and distributional nature, of the collected data were suitable for the purposes of analysis using the selected multivariate data analysis methods. Analysis of the data provided assurance that data collected possessed univariate normality, and indicated that the dataset was suitable for the purpose of multivariate data analysis. The objective of multivariate analysis is to produce evidence from the data to support or refute the relationships within, and the hypotheses based on the research model outlined in **Chapter 3** of this thesis.

8.1 Introduction

The multivariate analysis research consisted of several related processes of analysis in which the outputs of one set of techniques was used in, or to validate the use of, the following techniques. The preparatory processes used were bivariate correlation analysis, EFA, CFA to ensure that the measurement model was of sufficient reliability and validity to be used for structural analysis utilising SEM and its' associated multivariate analysis processes, detailed in the following sections.

8.2 Bivariate Correlation Analysis

Testing for normality using descriptive statistics and ANOVA were adequate to ascertain the univariate normality of the observations used in the modelling process. To minimise the possibility that the normality of the combined observations were unsuitable for the testing methods it was necessary to investigate the two-tailed bivariate correlation of the variables to ensure that any significant correlation between the constructs did not bias the results unduly.

8.2.1 Correlation Matrix

A bivariate analysis of the proposed constructs was used to produce the correlation matrix in Table 8.1, produced using the Pearson correlation coefficient to analyse the correlation between two datasets. The analysis suggests that multi-collinearity could have been present between the constructs of trust and reputation as evidenced by the relatively high bivariate correlation value of 0.782, and between trust and communication quality where the correlation was 0.797. These values are higher than the recommended threshold of 0.7 (Hair et al., 2010), and were attributed to the close theoretical relationship between the constructs. In the literature, trust and trustworthiness have sometimes been used wrongly and interchangeably (Hardin, 2002). As the communication of trustworthiness, reputation is likely to show high correlation, and communication quality, representing the passing of trust information between parties was also attributed to this close theoretical relationship.

Table 8.1 Construct Correlation Matrix

	Communication Quality	**Delegation**	**Outcomes**	**Information Security**	**Trust**	**Reputation**
Communication Quality						
Delegation	0.647					
Outcomes	0.701	0.604				
Information Security	0.616	0.609	0.596			
Trust	0.797	0.664	0.676	0.654		
Reputation	0.775	0.695	0.663	0.672	0.782	

8.2.2 Multi-Collinearity Detection

The correlation matrix (Table 8.1) revealed that the highest correlations between factors were between trust and communication quality (0.797) trust and reputation (0.781). Given these higher than expected values suggestive of multi-collinearity a process of detection was performed to ensure that the Tolerance and VIF values were below the recommended thresholds.

8.2.3 Tolerance and Variance Inflation Factor

Having established that a higher than recommended correlation between trust and reputation constructs existed, this observation was investigated by using SPSS to run multi-collinearity diagnostics. Tolerance and Variance Inflation Factor (VIF) measures were the two techniques used to assess the potential impact of multi-

collinearity on the analysis. Using the reputation construct as the dependent variable the correlation, tolerance and VIF were produced to aid the detection of potential multi-collinearity (Table 8.2).

Table 8.2 Collinearity Statistics

Collinearity Statistics*		
Construct	**Tolerance**	**Variance Inflation Factor**
Delegation	0.463	2.160
Communication Quality	0.453	2.210
Information Security	0.422	2.368
Outcomes	0.405	2.470
Trust	0.348	2.874

*Dependent Variable: Reputation

The tolerance and VIF calculation values confirmed that excessive multi-collinearity was not present between any of the constructs used in the model.

8.2.4 Bivariate Correlation Analysis Summary

Correlation analysis techniques were employed to discover the bivariate correlational attributes of the proposed constructs, and a multi-collinearity assessment was performed to ensure that the analysis was not unduly biased by the correspondence between constructs.

The constructs used in the research analysis revealed a higher than recommended correlation between trust and reputation but further investigation of

the tolerance and VIF values of the constructs did not suggest the presence of multi-collinearity. Reputation, trust, and communication quality are closely aligned theoretically by which measure the correlation would be expected to be high in established trust relationships, and the calculated correlation ratios suggest that these observations match the theory. However, by incorporating the constructs into the research model the covariance relationships subsequently confirmed by multivariate analysis suggested that the nature of trust and reputation are sufficiently differentiable to yield results without the bias effects of multi-collinearity.

In addition to determining the discriminant validity of the constructs the correlation analysis ensured that the data that had been obtained were sufficiently uncorrelated to allow orthogonal rotation methods to discover the factors using EFA, detailed in the next section.

8.3 Exploratory Factor Analysis

The suitability of employing EFA techniques to the data was obtained in part by calculating the critical ratios to test for multivariate normality (Section 7.5.8). The justification for employing multivariate techniques to the data was obtained by calculating the KMO test of sampling adequacy and Bartlett's test of sphericity. The values of 0.943 obtained for the KMO was above the 0.5 threshold for sample adequacy (Kaiser, 1974). The value of 0.000 for the Bartlett's test was significant and confirmed that the correlation matrix was not an identity matrix incapable of being analysed using factor analysis.

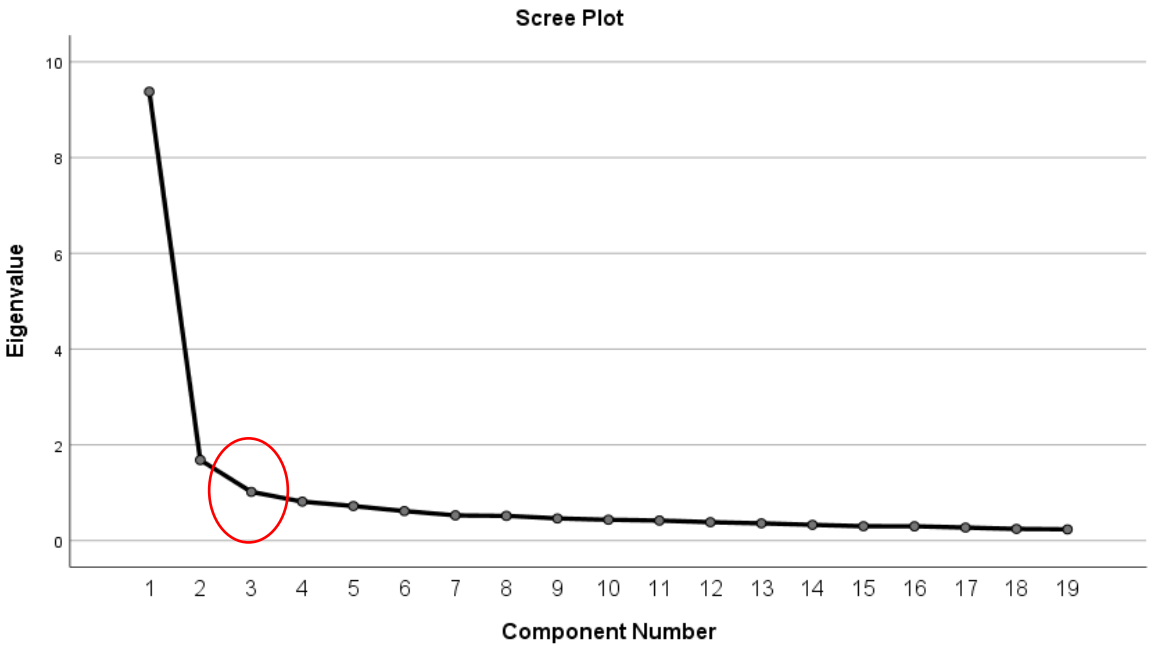
An initial EFA was carried out to detect the potential number of factors in the model. This analysis informed part of a post data collection construct and item purification recommended by Churchill (1979).

8.3.1 Factor Extraction

A scree plot of the latent root (eigenvalue) against the number of factors in order of extraction was used to evaluate the eigenvalues present in the analysis (

Figure 8-1). The Scree test was interpreted on the number of values that had eigenvalues >= 1.0 and this was chosen as the cut-off point as explaining the majority of the variance present within the results set. As the basis for the analysis was Factor Analysis rather than Principal Component Analysis it was possible to include the six research constructs as factors based on prior theory (Hair et al., 2010). This decision was strengthened by the correlation matrix results (Section 8.2.1) revealing higher than expected correlations between some of the factors. Having consolidated the data items of interest, the communality of the items were calculated.

Figure 8-1 Scree Plot



8.3.2 Communality

The results of the communality analysis are detailed in Table 8.3. The values obtained demonstrate that the variables selected for analysis using CFA display sufficiently high communalities, and therefore absorb sufficient variance to be good measurement indicators. The high communality displayed was required for factor rotation, a technique that was used to uncover the factor structure.

Table 8.3 Variable Communalities

Item and Item Coding	Initial	Extraction
SE1 - The organisation appears to value the importance of security.	1.000	.741
SE2 - Information security is a key normal behaviour of the organisation.	1.000	.784
CQ2 - The organisation will deal calmly and efficiently with any unexpected events.	1.000	.785
CQ1 - Any notifications I receive from the organisation are relevant and timely.	1.000	.791
CQ3 - Interaction with the organisation is generally constructive and supportive.	1.000	.719
TR1 - The organisation would not knowingly do anything to harm me.	1.000	.737
TR2 - I believe that the information privacy assurances offered by the organisation will be honoured.	1.000	.710
TR3 -I know that my information is safe and access is limited only to authorised personnel.	1.000	.703
RE1 - Sound principles seem to guide the behaviour of the organisation.	1.000	.767
RE2 - The organisation has a reputation for being honest.	1.000	.728
RE3 - The organisation has a reputation for looking after its patients/customers.	1.000	.719
DE1 - I trust the organisation enough to allow it to delegate the task of fulfilling my instructions to another person or information system.	1.000	.835
DE2 - I believe that if the organisation delegated tasks it was to help achieve my goals.	1.000	.812
DE3 - I can trust the organisation or their agent to act in my place.	1.000	.676
OC1 - Allowing the organisation to update records electronically /achieve the transaction gave me the confidence to engage with the same provider again.	1.000	.845
OC2 - I am able to give objective feedback to the organisation or the service provider.	1.000	.815

8.3.3 Factor Rotation

Although some correlation was present in the data (see Table 8.1 Construct Correlation Matrix), orthogonal rotation was chosen in preference to oblique rotation techniques to reveal the factor structure. Orthogonal rotations were used as the correlation and multi-collinearity analysis had determined that the constructs were not unusually highly correlated and did not display multi-collinearity. Varimax was

chosen as the method of rotation as the stated aim of the rotation process was to maximise the sum of variances represented by the factors, with the factors showing a clear separation. Varimax achieves this by minimising the number of variables that have high loadings on each factor.

After application of rotation the rotated component matrix was examined for significant factor/item loadings. Significant loadings were considered to be higher than 0.3 for the sample size of 405 observations (Hair et al., 2010). The matrix provided a starting point for the interpretation of factors based on the measurement variables. The highest loadings represent the variables most strongly associated with a factor. Some variables displayed significant cross-loading against more than one factor, and these cases the highest aggregated factor loadings were selected even though some variables indicated low significance. The variables selected for each factor are highlighted in Table 8.4 Rotated Factor Matrix.

Table 8.4 Rotated Factor Matrix

Rotated Component Matrix[a]						
	Component					
	1	**2**	**3**	**4**	**5**	**6**
The organisation should protect our relationship from cyber threats and their effects.	.108	.146	.069	.808	.032	**.227**
Information I have given to the organisation in one context should not be used in an unrelated context (e.g. research) without my permission or knowledge.	.122	.113	.008	.894	.146	**.071**
The organisation will deal calmly and efficiently with any unexpected events.	.328	**.739**	.172	.146	.164	.091
Any notifications I receive from the organisation are relevant and timely.	.227	**.777**	.175	.080	.244	.103
Interaction with the organisation is generally constructive and supportive.	.461	**.531**	.280	.306	.181	.132
The organisation would not knowingly do anything to harm me.	.387	.455	.187	**.217**	.084	-.168
I believe that the information privacy assurances offered by the organisation will be honoured.	.540	.492	.122	**.187**	.147	.112
I know that my information is safe and access is limited only to authorised personnel.	.586	.375	.133	**.078**	.256	.031
Sound principles seem to guide the behaviour of the organisation.	**.757**	.276	.196	.145	.107	.079
The organisation has a reputation for being honest.	**.636**	.209	.236	.077	.179	.019
The organisation has a reputation for looking after its patients/customers.	**.546**	.529	.306	.169	.072	-.006
I trust the organisation enough to allow it to delegate the task of fulfilling my instructions to another person or information system.	.136	.224	**.830**	.042	.158	-.056
I believe that if the organisation delegated tasks it was to help achieve my goals.	.312	.159	**.789**	.036	.094	.113
I can trust the organisation or their agent to act in my place.	.533	.411	**.415**	.018	.206	-.060
Allowing the organisation to update records electronically /achieve the transaction gave me the confidence to engage with the same provider again.	.087	.287	.230	.142	**.771**	.093
I am able to give objective feedback to the organisation or the service provider.	.513	.191	.098	.131	**.693**	.086
Rotation Method: Varimax with Kaiser Normalization.						
a. Rotation converged in 8 iterations.						

The rotation analysis was re-run for comparison using Direct Oblimin rotation to account for any oblique rotation that may be present. However, using this technique also meant that some of the variables deemed as significant by orthogonal rotation were no longer significant using oblique rotation, making the overall (aggregated) significance of each factor lower. It was concluded that the varimax rotation was the most robust significance rotation indicator method of the two analyses when data was aggregated at factor level.

8.3.4 Cronbach Alpha

The Cronbach α was calculated for the proposed factors as a preliminary measure of the internal reliability of the indicator constructs. Adjustments made to construct measurement by measurement reduction and item purification increased the ability to measure constructs consistently, whilst maintaining summated multi-item scales for all constructs to maintain reliability (Gliem and Gliem, 2003).

Table 8.5 Cronbach Alpha Reliability Scores

Construct	Number of Items	Overall	Scenario 1 (Retail)	Scenario 2 (Banking)	Scenario 3 (Medical)
Communication Quality	3	0.843	0.818	0.853	0.857
Delegation	3	0.798	0.717	0.822	0.843
Outcomes	2	0.698	0.702	0.698	0.616
Security	2	0.781	0.703	0.792	0.815
Trust	3	0.838	0.826	0.829	0.856
Reputation	3	0.833	0.780	0.852	0.852

Having established that the data contained discrete factors composed of variables, the factors were named to reflect the question items and to represent the factor's conceptual meaning. These names were used throughout the research to identify the model constructs that were derived from the factors.

The final item purified constructs that were used in the analysis (Table 8.5) all displayed Cronbach alpha reliability scores of > 0.7, with the exception of the outcomes construct, where the reliability was 0.62, but still considered to be an acceptable level for analysis. The reliability of the outcome construct suggested that there was a lower item-pair correlation between the post-hoc evaluation and feedback scores for delegated tasks in healthcare scenarios where credence attributes are more relevant to consumers than search and experience attributes (Darby and Karni, 1973). For most constructs and scenarios the values obtained for the Cronbach alpha coefficients were very close to, or over the threshold of 0.7, and all were above the recommended adequate level of 0.6 (Hair et al., 2010).

Calculating the alpha coefficient provided a pre-analysis indicator of reliability that considers each measure in the construct to have equal weighting, an assumption that is rarely met in real world observations. Cronbach's alpha also makes the assumption that all error measurements are uncorrelated, and is known to underestimate the reliability of congeneric measures (Raykov, 1997). The shortcomings of relying solely on the Cronbach's alpha as a single reliability measure were offset by subsequently calculating more accurate estimates of item loading and composite reliability as part of the CFA process (Section 8.4.1) to ensure that the

assumptions inherent in the Cronbach alpha calculation did not have any substantive effect on the analysis.

8.3.5 EFA Summary

The measurement model proposed from the conceptual research model was verified using Exploratory Factor Analysis (EFA) techniques to survey the model constructs. Factor analysis was used to identify the factors present in the data, and to uncover the structure and pattern of relationships between the factors and their relevant indicators. The identified factors were then used to represent the corresponding conceptual research constructs. The results obtained from the EFA techniques for factor analysis were cross checked with the hypotheses and the supporting academic literature to ensure that they corresponded with the theoretical viewpoints and were broadly consistent with the constructs proposed in the research model.

Factor extraction using the scree test confirmed that the number of factors extracted for analysis represented the most significant predictors of variance; communality analysis provided an indication of the variance each item was able to assimilate; and rotation using orthogonal and oblique rotation ensured that the measures used in the factors had the highest loadings. These EFA techniques were used to test the strength of the research constructs based on common factor analysis, and to confirm the significance of the measures and constructs subsequently used in the CFA process detailed in the next section.

8.4 Confirmatory Factor Analysis

The measurement model was confirmed and tested using Confirmatory Factor Analysis (CFA). In CFA the researcher specifies the number of factors and the pattern of indicator-factor loadings in advance as well as other parameters such as those bearing on the independence or covariance of the factors and indicator unique variances. These techniques established the item convergence and discriminant validity of the chosen constructs. Taken together, both the EFA and CFA analyses contribute to measures of reliability and validity (Rossiter, 2002).

The analyses that were performed to ensure that the validity and reliability of the measurement model included a consideration of item loadings to the factors, the correlation between factors and an assessment of the Composite Reliability and Average Variance Extracted by the factors, which are detailed in the following sections.

8.4.1 Item Loadings

The factors were tested to confirm that they were supported by high item loadings that exceeded the threshold of 0.50 (Hair et al., 2010) and were significant for analysis purposes (Table 8.6). Where items contributed to more than one factor and cross correlation between items occurred, the items were removed from the analysis to ensure that the items represented sufficient uni-dimensionality of meaning (Anderson and Gerbing, 1988; Jöreskog and Sörbom, 1984).

The strong item loadings obtained of >0.64 independently supported the framework of prior academic work in the area of cybersecurity, trust and task delegation that were used to derive the question variables.

Table 8.6 Item Loadings

Factor	Item	Item Loading
Communication Quality	CQ1 -I receive relevant and timely notifications from the organisation.	0.77
	CQ2 -The organisation will deal calmly and efficiently with any unexpected events.	0.82
	CQ3 -Interaction with the organisation is generally constructive and supportive.	0.81
Delegation	DE1 -I trust the organisation enough to allow him/ her to delegate the task to another person or information system.	0.71
	DE2 -I believe that delegating the task will achieve my task goal.	0.75
	DE3 -I can trust the delegated agent to act in my place.	0.78
Outcomes	OC1 -Achieving the transaction gave me the confidence to engage with the trustee again	0.70
	OC2 -I am able to give objective feedback to the service provider.	0.70
Security	SE1 -I feel that the organisation appears to value the importance of security.	0.83
	SE2 -Information security is a key normal behaviour shared between myself and the organization.	0.78
Trust	TR1 -The organisation would not knowingly do anything to harm me.	0.76
	TR2 -I know that my information is safe and access is limited only to authorised personnel.	0.82
	TR3 -I believe that the information privacy assurances offered by the organisation will be honoured.	0.81
Reputation	RE1 -The organisation has a reputation for being honest.	0.78
	RE2 -Sound principles seem to guide their behaviour.	0.78
	RE3-The organisation has a reputation for looking after its customers.	0.79

8.4.2 Composite Reliability (CR) and Average Variance Extracted (AVE)

Use of the Cronbach alpha measure of reliability was strengthened by utilising the factor analysis loadings obtained from the CFA analysis to calculate each constructs' composite reliability and AVE (Table 8.7), representing the reliability calculated by the contribution of each item and the amount of variance captured by

the construct in relation to the amount of measurement error variance respectively (Fornell and Larcker, 1981).

All of the composite reliability calculations were above the threshold of 0.7, and all of the AVE calculations were above the threshold of 0.5, adding further evidence of reliability and convergent validity.

Table 8.7 Composite Reliability and Average Variance Extracted

Construct	Composite Reliability (CR)	Average Variance Extracted (AVE)
Communication Quality	0.83	0.64
Delegation	0.79	0.56
Outcomes	0.70	0.54
Security	0.78	0.64
Trust	0.84	0.64
Reputation	0.83	0.62

8.4.3 *R^2 Values*

The values obtained for the R^2 of the model factors are shown in Table 8.8. The values were found to be greater than the threshold of 0.5, below which they would only have accounted for the variance by chance (Hair et al., 2010). This indicated that the factors were able to explain a high proportion of the variance of in a regression model that included the security construct as the independent variable.

Table 8.8 R^2 Values

Factor / Construct	Full Model	Retail	Banking	Healthcare
Reputation	0.71	0.79	0.64	0.78
Trust	0.95	0.87	0.97	0.99
Communication Quality	0.90	0.88	0.87	0.94
Delegation	0.76	0.74	0.59	0.88
Outcomes	0.74	0.95	0.79	0.84
* Independent Variable Security				

8.4.4 *CFA Summary*

The logical research model, verified by use of the EFA analysis techniques was further developed by the application of item loadings to ensure that the chosen research question responses provided significant weight to the constructs. Combining these item loadings with the prior calculations of the Cronbach Alpha reliability measures provided further scale purification which resulted in some of the final questionnaire items being dropped from the model.

This resulted in higher AVE and R^2 values for the constructs in the research model. As a result of calculating the composite reliability values the proposed construct of confidentiality was dropped from the refactored model. This was done to provide further purification of logically related items that did not display the convergent validity necessary to provide sufficient reliability to provide evidence to support the model. The further purified model constructs were employed in Structural Equation Modelling analysis, detailed in the next section.

8.5 Structural Equation Modelling

Covariance Based Structural Equation Modelling (CB-SEM) was used to investigate and test the nature of the structural model based on fully saturated structural model. An iterative process of model trimming and testing was employed to ensure that the covariance model fitted the proposed construct relationships. The modelling process followed the Anderson and Gerbing (1988) two-step process by firstly ensuring that the research model was assessed as possessing adequate fit to the data. The second step of the process involved further fitting of the model by comparison to equivalent models with constrained and unconstrained parameters to reach an optimum solution displaying a low Model Chi square (χ^2_m) and a maximum number of degrees of freedom.

8.5.1 Sample Size

The sample size required to effectively utilise Structural Equation Modelling is the subject of academic discussion (Iacobucci, 2010). Sample size is not important for identifying a path model, but in common with other statistical techniques the results from larger samples experience less sampling error than smaller samples. One method of sample sizing using the observations to item ratio ensured that the factor loadings were sufficient for analysis. The estimates of numbers required vary and relevant sample size considerations for SEM suggest sample size should also be based on five characteristics. These are the multivariate normality of the sample; the estimation technique used; the model complexity; whether any data is missing; and the average

error variance (communalities) of indicators (calculated as the square of the standardised construct loadings) (Hair et al., 2010).

Based on these recommendations a sample size of 150 is recommended for models with seven or fewer constructs, modest communalities (0.5), and no under identified constructs. The nature of the research dataset used met these recommended criteria values. The data set was characterised by moderate to good multivariate normality allowing MLE methods to be used. The proposed research model was of medium complexity with six constructs and seven paths, no missing data, and an average communality of 0.77. This lead to the conclusion that a sample size of at least 150 was required for the proposed analysis. The actual number of questionnaires completed and cleansed (*n*=405) counted as a large sample. The larger sample size is recommended to aid more complex modelling (Kline, 2005) and to provide a more stable solution (Hair et al., 2010). The completed questionnaires for the scenarios also provided an adequate sample (*n*=133/136/136) to effectively utilise SEM analysis techniques in each of the contexts.

8.5.2 Model Fit

As described in the research methods chapter (Section 6.6, SEM Model Fitting) fit indices were calculated to provide an indication of the overall fit of the model to the observed data. As aggregate measures of goodness-of-fit they may give overall good values even when portions of the model have a poor fit. Achieving a good fit does not necessarily reflect that the model makes theoretical sense, and does not

guarantee that the model is correct. Fitting a model well requires that the preparation of the sample data and the measurement is rigorously undertaken.

The sample size was deemed to be of sufficient size (*n*=405) to provide stability and for model fitting indices to work reliably. The descriptive statistics (**Chapter 7, Descriptive Data Analysis**) indicated that the data were of adequate normality for the Maximum Likelihood method of parameter estimation to provide adequate estimates of path co-variances.

The judicious use of indices provided calculated numbers to summarize the fit to guide the reasoning behind selecting the most appropriate interpretation of the co-variances present. The iterative model trimming strategy employed for testing ensured that the best possible fit of RMSEA, Fit indices, and minimum Chi squared results were obtained, balancing sample based indices, parsimony-based indices and information theory indices with the insights from previous theoretical work to ensure the optimum model fit.

Table 8.9 Overall CFA Model Fit Summary

Confirmatory Factor Analysis *n*=405		
Fit index	**Values**	**Fit Analysis**
χ^2 / df / (χ^2/df) ratio (NC) /p	268.260/98/3.014	Good
NFI/RFI/IFI/TLI/CFI	0.936/0.914/0.956/0.941/0.956	Good
RMSEA/LO90/HI90/*p*close	0.071/0.061/0.080/0.000	Good
SRMR	0.0364	Good
AIC	394.260	N/A

Table 8.10 Overall SEM Model Fit Summary

Structural Equation Model *n*=405		
Fit index	**Values**	**Fit Summary**
χ^2 / df / (χ^2/df) ratio(NC) /p	278.624/98/1.835/0.000	Good
NFI/RFI/IFI/TLI/CFI	0.934/0.919/0.956/0.946	Good
RMSEA/LO90/HI90/*p*close	0.068/0.058/0.077/0.001	Good
SRMR	0.0365	Good
AIC	477.435	N/A

The CFA and SEM models displayed the fit indices in Table 8.9 and Table 8.10. The analysis of model fit indicated by the index values reported is based on the generally accepted threshold values for the indices discussed in Section 6.6, SEM Model Fitting . The values obtained suggest that the research model represents an adequate to good closeness of fit to the research data.

8.5.3 Path Coefficients

Model paths represent the structural relationships that are present between latent constructs. Depicting a model with multiple interconnecting paths between the nodes leads to increasing model complexity. The theoretical considerations relevant

to the research domain, as described in the Literature Review section of this thesis were used in identifying which relationships were more likely to be present. Limiting the paths to be estimated by identifying only the most salient relationships ensured that an over-identified recursive research path model was obtained with which to evaluate the research hypotheses.

The software package used to evaluate the relationships utilised Maximum Likelihood estimation techniques to iteratively calculate the best fit for the path model to the observed data. The standardised regression coefficients (β) obtained as a result of parameter estimation are detailed in Table 8.11.

Table 8.11 Path Coefficients

Path	**Hypothesis**	β	***p*-value**
Information Security → Reputation	H1	0.853	p<0.0001
Reputation → Trust	H2	0.971	p<0.0001
Trust → Communication Quality	H3	0.944	p<0.0001
Reputation → Delegation	H4	0.875	p<0.0001
Communication Quality → Outcomes	H5	0.698	p<0.0001
Delegation → Outcomes	H6	0.187	p = 0.081

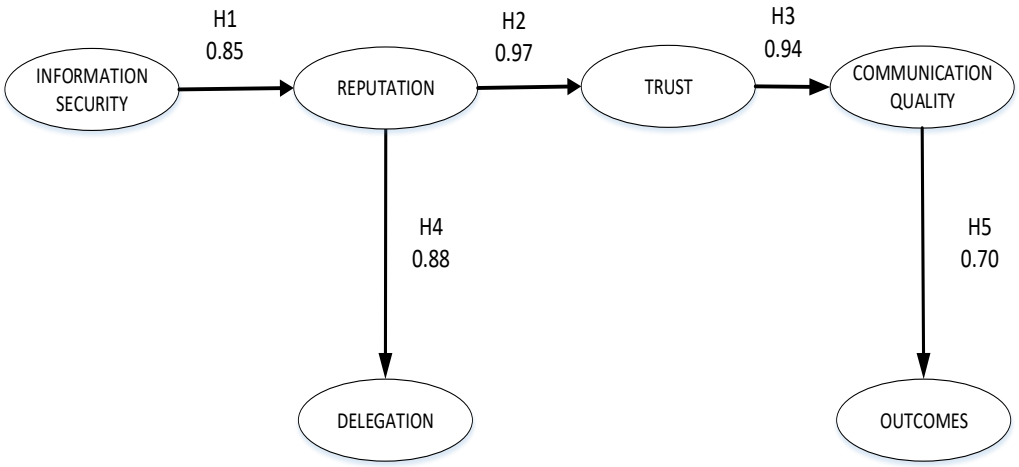
**n*=405

The coefficients obtained from path analysis of the full dataset confirm the research hypotheses H1 to H5 with varying degrees of correspondence to the observed data. Hypothesis H6 was not supported by the data and was rejected.

8.5.4 Hypothesis Testing

The path model that represented the best fit to the observed data is included in Figure 8-2

Figure 8-2 Model Standardised Beta Values



The paths in the accepted model represent the hypotheses that were posited in **Chapter 3, Conceptualisation**, with the exception of Hypothesis H6 that was not significant. As such, the acceptance of the model, and the β covariance coefficients that comprise it provided inferential statistical evidence that was used to test the validity of the claims made in this research dissertation.

Testing the paths, and therefore the hypotheses associated with them confirmed H1, that information security has a strong positive correlation with reputation ($\beta=0.843$, $p<0.0001$) and the hypothesis was supported. This path represents the connectedness of the cybersecurity variable with those of the trust domain.

Hypotheses relating to the interconnectedness of the cognitive trust variables was also found. Support was demonstrated for hypotheses H2, that reputation and trust are positively related, ($\beta=0.974$, $p<0.0001$) and H3, that trust and communication quality are correlated ($\beta=0.887$, $p<0.0001$). These demonstrated strong covariance relationships that reinforce previous theoretical and empirical work in the area of trust.

The behavioural components of trust, in delegation and the evaluation of outcomes were found to be partially supported by the model. Support for H4, that reputation and delegation are positively correlated, ($\beta=0.876$, $p<0.0001$) was a strongly supported hypothesis. Hypothesis H5, that there is a positive relationship between communication quality and outcomes ($\beta=0.704$, $p<0.0001$) was also strongly supported by the analysis. However, hypothesis H6, that delegation and outcomes were positively related to each other ($\beta=0.187$, $p=0.081$) was not significant and so was rejected. This finding suggests that the outputs of delegated action are not necessarily related to the outcomes of the actions taken. Trusting communication quality does not appear to correlate directly with the results of actions taken, suggesting that there is a missing variable in the relationship between delegation and

outcome, as theory states that only in cases of blanket trust is the link between actions and outcomes disregarded.

8.5.5 SEM Model Fitting Summary

That SEM can produce many different validated models has been noted in the literature (Hair et al., 2010). Therefore, in choosing a validated model from a selection means that the criteria for using one model over another must be investigated. As part of the testing strategy, iterative model trimming was performed on both the measurement and structural models to ensure parsimony of variables and goodness-of-fit.

The strongest indicator of whether a model is a good fit is that it displays the lowest Chi-squared value, as this shows the model has been able to absorb the most variance between the actual and predicted model. Chi-squared is, however, susceptible to population and sample size effects, so other measures that take into account the parsimony of fit must also be considered. Information theory models were also used to select the final validated model that best represented the theoretical grounds for research, so that where competing models represented a similar fit and the model with the lowest AIC value was selected.

After model selection, the paths represented in the model were used to accept the initial research hypotheses based on the beta coefficients obtained from the structural equation analysis. Having accepted that the full research model represented a good model fir to the data, it was possible to evaluate whether the accepted model

was a good aggregate fit across all the contexts tested using the scenario datasets. The results of this process are presented in the next section.

8.6 Model Stability

Having established that the measurements produced good structural goodness-of-fit across all scenarios, invariance insights were applied to the measurement model to ensure that testing in each of the scenarios (Retail, Banking and Healthcare) in turn presented an acceptable chi-square value and fit index values that were able to support the findings of the generalised all scenario model across the different contexts.

8.6.1 Measurement Invariance

To generalise the stability of the structural model across different contexts it was necessary to first ensure that the measurements used to evaluate the model were invariant across these contexts and that they did not represent different concepts to the respondents that provided their opinions. This was achieved by using the techniques of multiple group confirmatory factors analysis (MGFA), as described in **Section 6.7.1, Measurement Invariance**.

The results of invariance testing are detailed in Table 8.12. Fit indices for the measurement model were found to have configural invariance across the three separate scenarios tested showing that the same basic factor structure existed, and demonstrating that the constructs were congeneric across the groups. This produced

the totally free (unconstrained) group model that was used for baseline comparison purposes.

The second round of testing was able to establish measurement weight invariance through proving the equivalence of the factor loadings (weights) to each construct. This established that the equivalence was present by setting the factor loadings that represent the relationship between the indicators and the latent construct to be equal. By determining that the factor loadings were equal across the groups, and the χ^2 p-value was not significant it provided evidence that the constructs retained their 'meaning' across the scenarios.

Table 8.12 Measurement Invariance Tests

	Model Fit Measures					**Model Differences**		
Model	**χ^2**	***df***	**P**	**RMSEA**	**CFI**	**$\Delta\chi^2$**	**df**	**P**
Separate Groups								
Retail	166.0	89	.000	.081	.933			
Banking	222.9	89	.000	.106	.911			
Healthcare	175.1	89	.000	.085	.948			
Unconstrained Model	564.0	267	.000	.053	.931			
Measurement Weights	584.8	287	.000	.051	.931	20.8	20	.000
Measurement Intercepts	751.5	319	.007	.058	.899	166.6	32	.007
Structural Covariances	819.1	361	.023	.056	.893	67.6	42	.016
Measurement Residuals	895.1	393	.066	.056	.883	76.0	32	.043

The measurement intercept invariance was calculated by constraining the variable intercepts on the construct, allowing the relative amounts of the latent constructs between groups to be estimated. The results showed that the model did

possess measurement intercept invariance, the χ^2 value was higher but the p values and CFI fit index were still sufficient to support the model when the constraints were applied. The model also displayed structural covariance invariance whereby the constructs were constrained to ensure that they are related to each other in a similar fashion across groups. However, the measurement residual variances displayed not only significant χ^2 values, but this was were accompanied by increases in the *p*-value and a deterioration in the CFI fit index.

Therefore, the model was able to achieve partial invariance (measurement weight and intercept) without a significant difference. This ensured that the factor structure and the factor loadings were sufficiently invariate for the purposes of SEM context model stability testing detailed in the next sub section.

8.6.2 Context Model Stability

The constructs did not display significant variance between scenarios as evidenced by the measurement invariance found in the previous section. The fitted full model was retested with a subset of observations that related to each scenario. The presence of a level of measurement invariance returned fit indices that confirmed the model still corresponded to the data. The values relating to the different scenarios and the full model fitting indexes for reference are shown in Table 8.13.

Table 8.13 Model Stability Indices

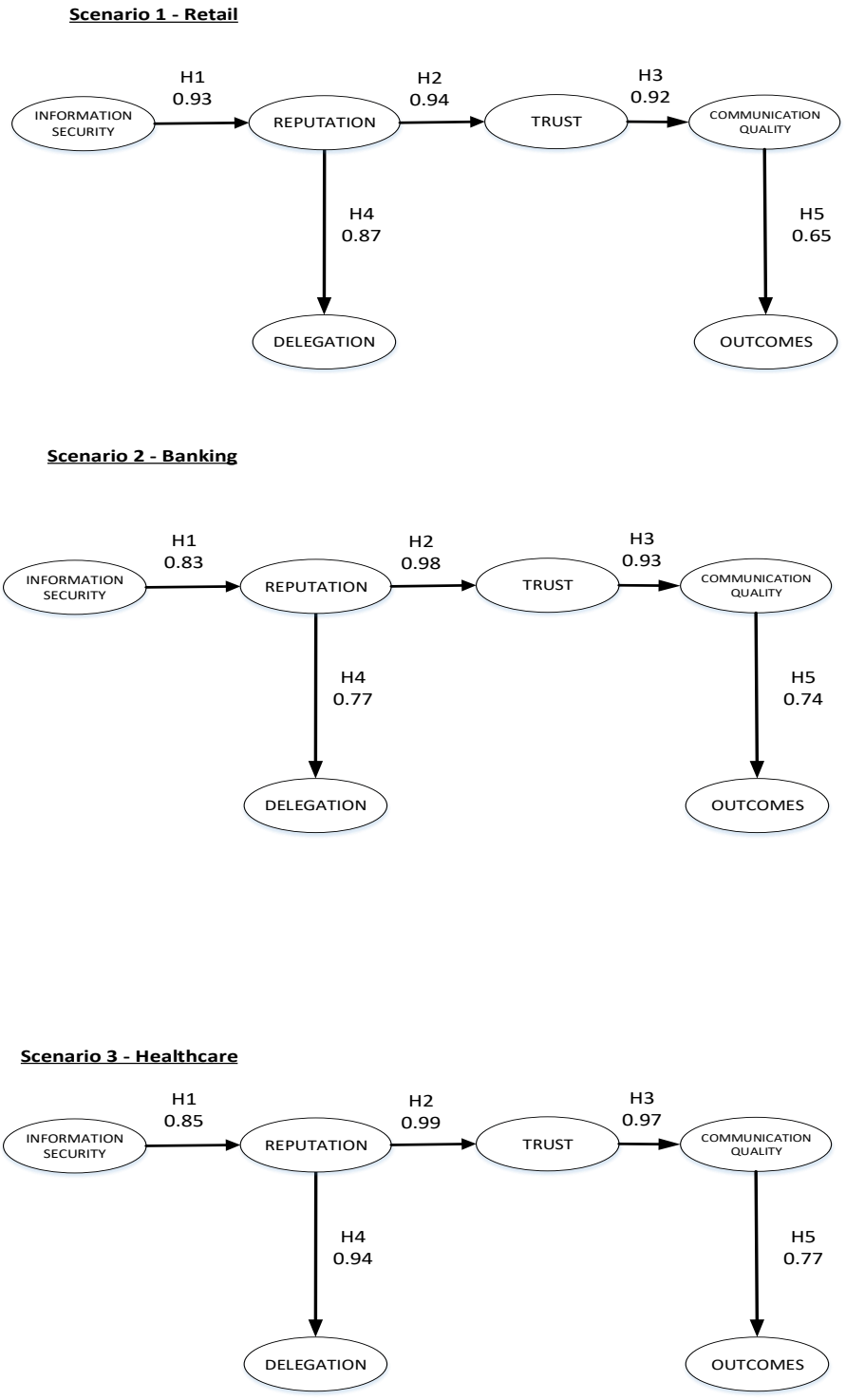
Structural Equation Model				
Scenario (*n*=)	**X^2 / df / (X^2/df) ratio /*p***	**NFI/RFI/IFI/TLI/CFI**	**RMSEA/LO90/HI90**	**AIC**
Online Retail (133)	179.9/98/1.835/0.000	0.858/0.826/0.930/0.929	0.08/0.061/.098	287.873
Online Banking (136)	236.5/98/2.414/0.000	0.854/0.822/0.909/0.887/0.908	0.102/0.086/0.119	344.561
Healthcare (136)	198.8/98/2.024/0.000	0.888/0.863/0.940/0.925/0.939	0.087/0.070/0.105	306.344
Full Model (405)	278.624/98/2.843/0.000	0.934/0.919/0.956/0.946/0.956	0.068/0.058/0.077	386.624

Model fit indices for the scenarios are weaker than the indices for the full model, displaying lower fit values than the composite data set. This is due in part to the smaller data sets used, as the number of observations (*n*=133 /136) are marginally smaller than the recommended values of 150 for the size and complexity of the model being tested (Hair et al., 2010). The smaller number of observations result in a penalty for measures, for example the RMSEA, and where the fit index compares to a baseline model (NFI/RFI) the relative lack of values may lead to asymmetry that will also reduce the index.

Path analysis of the models fitted to each of the three scenarios (Figure 8-3) showed that the standardised beta values supported the hypotheses at the level of individual contexts, confirming the measurement invariance exercise carried out in **Section 8.6.1**. Variations were observed between the scenarios in several areas:

- **Retail.** In this scenario the covariance relationship between Reputation and Delegation was higher (0.93) and the covariance between communication quality and outcomes was lower (0.65).

Figure 8-3 Context Model Standardised Beta Values



- **Banking.** The covariance between Communication Quality was higher (0.74), and the relationship covariance between Reputation and Delegation was lower (0.77) than in the full information model.
- **Healthcare.** The relationship covariance between Communication Quality and Outcomes was higher (0.77) as was the covariance between Reputation and Delegation (0.94) compared to the full model.

A fuller account of the implications are included in **Chapter 9, Discussion and Conclusion**.

8.6.3 Model Stability Summary

In scenario based questionnaire research it is prudent to conduct further testing to give assurance that the model and its' constructs are measuring the same structures and meanings associated with the observations. This was achieved by executing multi-group analysis on the measurement model using multi-group CFA, and on the structural model using multi-group SEM. The CFA analysis concluded that the measurement model displayed configural and metric invariance, thus achieving a partial invariance that was deemed sufficiently strong to permit the use of multi-group SEM structure testing.

The SEM analysis on the scenarios, and the fit indices obtained, demonstrated that the full, aggregate model could be split into its' component scenarios and still

display adequate fit, and consequently, the explanatory power to draw conclusions about the connection between information security and trust in all of the research contexts, severally and separate. Having established the statistical veracity of the full model and the stability of its' constituent contexts, further path analysis techniques of mediation and moderation analysis were performed to bring further insight into the mechanisms of how and when the constructs in the model combined to produce the observed effects. The application of these methods are documented in the next section.

8.7 Mediation and Moderation

Fit indices to assess the overall goodness-of-fit to the observations were used to validate the research model at the structural level and the use of path analysis techniques established the existence of covariance relationships between the individual constructs. Once the association had been evidenced, the focus of investigation moved from establishing existence towards understanding the mechanisms by which its' effects operate and delineating the boundary conditions. The questions of 'how' and 'when' result in a deeper understanding of the relationships in the area of investigation and this knowledge was gained by executing mediation and moderation analysis on the tested model.

The classification of the relationship between independent and dependant variables using simple mediation gave a coarse indication of the presence of mediation in a relationship. The presence of partial mediation suggested the possibility that

variables involved in mediation may not be included in the model constructs, or the effects are suppressed (Rucker et al., 2011), a finding not uncommon in social psychology research.

8.7.1 Mediation Analysis

The analysis of the results of the Normal Theory testing is summarised in Table 8.14. The results show the full mediation effects of some relationships, and the presence of either no mediation, or only partial mediation present in other relationships. Therefore, the initial mediation results were further refined in a second round of asymmetry corrected bootstrapped tests to verify the findings and uncover further details about the mediation in model relationships. These methods were used to obtain the results in Table 8.15. The analysis and categorisation of the tests was carried out using the Zhao et al (2010) taxonomy of mediation, and the implications of the mediation relationships is detailed in Table 8.16.

Table 8.14 Normal Theory Mediation Analysis

Relationship	**Direct Effect Without Mediation**	**Direct Effect With Mediation**	**Normal Theory (NT) Analysis**
Security →Reputation→ Delegation	0.736(<0.001)	0.007(0.944)	Full Mediation
Security → Reputation→ Delegation→ Outcomes	0.128(0.176)	0.079(0.423)	No Mediation
Security→ Reputation→ Trust→ Communication Quality	0.851(<0.001)	0.209(0.034)	Partial Mediation
Security→ Reputation→ Trust	0.839(<0.001)	0.137(0.088)	Full Mediation
Reputation→ Trust→ Communication Quality	0.717(<0.001)	0.257(0.437)	Full Mediation
Reputation→ Trust→ Communication Quality→ Outcomes	0.848(<0.001)	0.355(0.001)	Partial Mediation

Relationship	**Direct Effect Without Mediation**	**Direct Effect With Mediation**	**Normal Theory (NT) Analysis**
Reputation→ Delegation→ Outcomes	0.344(0.002)	0.218(0.213)	Full Mediation
Trust→ Communication Quality→ Outcomes	0.682(<0.001)	0.195(0.242)	Full Mediation

A synthesised review of the results found that there was a high degree of correspondence between the results. The asymmetric bootstrapping values provided more fine grained insight into the nature of the mediation. This analysis also confirmed where no mediation was present. The analysis identified indirect-only mediated variable relationships, where the mediator was found to exist without a direct effect between the independent and dependent variables. The analysis also identified complementary mediation paths where both the direct and the indirect mediated path were both present and acting in the same direction.

Table 8.15 Mediation using Asymmetry Correcting Estimation

N=405, 2000 bootstrapped samples. Confidence intervals=Standardised Bias corrected 95% confidence intervals. ** = Values are significant at p< 0.01

Mediation	**Independent Variable (IV)**	**Dependent Variable (DV)**	**Direct Effect Estimate**	**Direct Effect Lower – Upper (Significance)**	**Indirect Effect Lower- Upper (Significance)**	**Asymmetry Corrected Analysis**
Security →Reputation→ Delegation	Security	Delegation	0.21**	-0.143 , 0.542 (0.222)	0.288,0.921 (0.001)	Indirect-only mediation.
Security → Reputation→ Delegation→ Outcomes	Security	Outcomes	-	0.157,0.410 (0.030)	0.056,0.642 (0.025)	No mediation.
Security→ Reputation→ Trust→ Communication Quality	Security	Communication	-	-0.087,0.410 (0.272)	0.355,0.833 (0.019)	No mediation.
Security→ Reputation→ Trust	Security	Trust	0.83**	-0.154,0.405 (0.235)	0.494-0.992 (0.001)	Indirect-only mediation.
Reputation→ Trust→ Communication Quality	Reputation	Communication	-	-1.697,1.362 (0.675)	-0.400,2.604 (0.136)	No mediation.
Reputation→ Trust→ Communication Quality→ Outcomes	Reputation	Outcomes	0.62**	0.017,0.606 (0.037)	0.225,0.756 (0.001)	Complementary mediation.
Reputation→ Delegation→ Outcomes	Reputation	Outcomes	0.68**	0.238,1.142 (0.005)	-0.246,0.464 (0.486)	No mediation.
Trust→ Communication Quality→ Outcomes	Trust	Outcomes	0.30**	-0.970,0.606 (0.117)	0.250,0.877 (0.001)	Indirect-only mediation.

In summary, the following mediation relationships (Table 8.16) were found to be significant.

Table 8.16 Mediation Relationships Summary

Relationship	**Mediation Effect**	**Implication**
Security → Reputation →Delegation	Full Mediation	Reputation has a significant mediating role between information security and task delegation.
Security → Reputation → Trust	Full Mediation	Reputation fully mediates between information Security and Trust. The reputation of a provider is a critical component in whether information security assurances result in trust.
Trust → Communication Quality → Outcomes	Full Mediation	Communication Quality fully mediates the relationship between trust and outcomes. The benefits of trust in the relationship are conferred due to the presence of the improved communication.
Reputation→ Trust→ Communication Quality→ Outcomes	Complementary Mediation	The constructs work in the same direction to work towards outcomes for the trusting parties.

8.7.2 Moderation Analysis

The introduction of moderator variables into the critical relationship in the research model, namely Security→ Reputation → Delegation was performed to discover the role of the theoretically most relevant variables of Cyber-awareness and Privacy Sensitivity in the strength and operation of the relationships between the cybersecurity construct, the cognitive trust constructs and the behavioural trust constructs. The methods used to derive the 'moderated mediation' effects of variables are described in the Moderation effects detailed in Section 6.8.3.

The results of the moderation analysis are recorded in

Table 8.17 and the simple first and second stage moderation effects calculated are shown in Table 8.18. The moderating variables of Cyber Awareness and Privacy Sensitivity were dichotomised into two groups for the purposes of analysis, based on whether respondents were higher in awareness or sensitivity (1 standard deviation above mean), or lower in awareness or sensitivity (1 standard deviation below mean).

Table 8.17 Moderating Variable Analysis

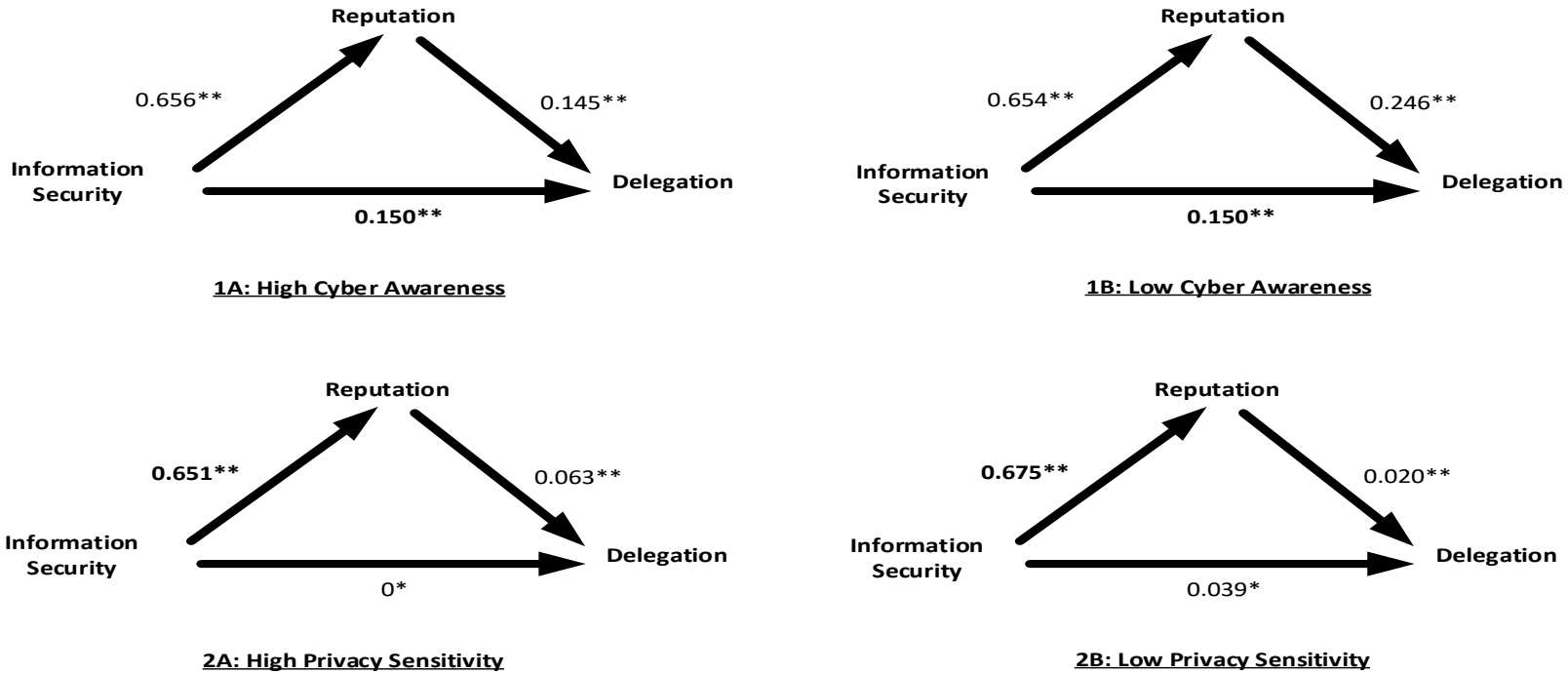
Moderator	IV Effect	MOD Effect	IV*MOD Effect	R^2	IV Path B	MED Effect	MOD Effect	IV*MOD Effect	MED *MOD Effect	R^2
Cyber Awareness	0.655 **	0.15	0.0001	0.45	0.263 **	0.524 **	0.004	-0.058	0.099*	0.56
Privacy Sensitivity	0.666 **	-0.05	0.132	0.46	0.260 **	0.516 **	-0.01	-0.23	0.124**	0.53
n=405, 2000 bootstrapped samples. Confidence intervals=Standardised Bias corrected 95% confidence intervals. Values are significant at *p<.05,**p< .01.										

Table 8.18 Moderator Effects at First and Second Stages

Moderator Variable	Stage		Effect		
	First	Second	Direct	Indirect	Total
Cyber Awareness					
High	0.655**	0.145**	0.80**	0.15	0.95
Low	0.654**	0.246**	0.262**	0.15	0.41
Differences	0.001	-0.101	0.062	0	0.54
Privacy Sensitivity					
High	0.651**	0.063**	0.714**	0	0.714
Low	0.675**	0.020**	0.695**	0.039	0.734
Differences	-0.024**	0.043	0.019	-0.039	0.20
n=405, STDDEV Cyber Awareness=1.0563, Privacy Sensitivity=0.8455.Significance at * *p* <.05, **p<.01.					

*The path values for Table 8.18 were calculated for path a as being the IV coefficient for the path + (Moderated IV coefficient)*StdDev for the stage 1 results, and for path b as the Mediator coefficient + (Moderated Mediator coefficient)*StdDev. The direct effect (path c) was calculated as the (IV coefficient)+ (Moderated IV)*StdDev. The indirect effects were calculated as being the sum of the moderation coefficients (path a + path b), and the total effect was the sum of the direct and the indirect path coefficients.

Figure 8-4 Moderation Effects of Cyber Awareness



Model 1 : Model showing simple effects for low and high cyber awareness moderator applied to the mediated relationship between security and delegation.
Model 2 : Model showing simple effects for low and high privacy sensitivity moderator applied to the mediated relationship between security and delegation.
Coefficients in boldface are significantly different (p<.05) across the moderator variable.
* p is significant at <.05, **p is significant at <.01.

The summarised moderation results are shown in Figure 8-4. The effects of the moderator Cyber Awareness on the relationship between security and delegation (Models 1A and 1B) were greatest in the path mediated by reputation for both high and low awareness users. There was with little effect on the relationship between the security and delegation. This finding suggests that users with all levels of awareness of cyber issues will rely more on the security credentials of a digital provider to assess the reputational trustworthiness of a provider prior to task delegation.

The moderating effect of Privacy Sensitivity on the relationship had no effect on the relationship between security and delegation. This was less significant than the effect on the relationship between security and reputation, the mediating variable in the relationship. This suggests that respondents with low and high privacy sensitivity will also rely on the reputation aspects of the relationship when delegating.

8.7.3 Mediation and Moderation Summary

Performing mediation path analysis using both normal theory methods and bias corrected bootstrap methods provided additional insight into the mechanisms by which the research model explains the workings of cybersecurity and trust in digital environments. It provided evidence that:

- Reputation fully mediates the relationship between information security and delegation.
- Reputation fully mediates the relationship between information security and trust.

- Trust and communication quality mediate the relationship between reputation and outcomes, with both effects acting in the same direction.
- Communication quality provides indirect mediation between trust and the outcomes of delegated behaviour.

The key relationship in the model that underpins the association between cybersecurity and trust is indicated by the observed co-variances between security and delegation, a relationship that is fully moderated by the reputation of the organisation. The investigation assessed whether moderating variables were acting on the relationship to influence when the associations are strongest. The moderating influence of both cyber awareness and privacy sensitivity were found to act directly on the security to delegation relationship, with both acting as positive moderators on reputation which, in turn, mediates the relationship between information security and delegation.

In providing these additional insights into the nature of the information security and trust relationship the use of mediation and moderation analysis provided further insight into the relationship between security and behaviour. The implications of the mediation and moderation findings are fully assessed in **Chapter 9, Discussion and Conclusion**.

8.8 Multivariate Data Analysis Chapter Conclusion

The steps taken as part of the multivariate analysis of the survey data were used to convert the raw observations into a fully fitted and tested model. The relationships within the model were further examined to uncover patterns in the observations to warrant the claims

of this thesis. Sample outputs of the analysis models are included for reference in **Appendix A3**.

Initial EFA was used to seek the underlying common factors to discover the structure of the dataset. These factors were used to build the constructs from which the model was formed. Reliability analyses were employed to ensure the internal construct reliability with which to underpin the validity of the constructs. Correlation analysis was performed to ensure discriminant validity and aid multi-collinearity detection to reduce bias in the analysis. CFA provided detailed item loadings and calculated further measures of construct reliability and discriminant validity.

CB-SEM tested the relationships between the reliable, validated constructs. The research model was trimmed and fitted, and measures of goodness-of-fit were applied, resulting in acceptance of the full model. This model was then tested for stability across the three research contexts, and the techniques of path analysis were used to assess the acceptance of the research hypotheses. Additional testing using several techniques was carried out to provide evidence of mediating and moderating variables that acted on the key paths within the accepted research model to provide additional evidence to support the thesis.

The multivariate analyses strengthen the findings and implications for practice that are presented in the following chapter, **Chapter 9, Discussion and Conclusion** by converting the raw observations obtained from the research survey into inferential statistical evidence.

9. Findings and Discussion

This thesis on the nature of information security and trust formation produced contributions to knowledge in terms of the development of theory in trust and cybersecurity, as well as contributions to the field of management, with both general and specific context applicability. The research approached the problem space by taking a structured, mixed methods approach to investigating the research problem.

9.1 Research Hypotheses and Discussion

The covariance of the research constructs were tested using the questionnaire responses received using SEM techniques, and these are detailed in **Chapter 8, Multivariate Data Analysis.** It was found that the relationships predicted by the model were correct. The null hypotheses were rejected and the covariance relationships proved are shown in Table 9.1.

A major new finding from these results was that there is a strong positive covariance relationship (β=0.853) between Information Security effects and Reputation effects. It is important because this relationship joins the cybersecurity field of enquiry to the trust field of enquiry. Information security and reputation are separate constructs that share a positive covariance relationship. This research has produced evidence that when organisations signal that they value trustee information, and adhere to the norms of shared behaviour with respect to information security, then the reputation of the organisation is strengthened. This,

in turn, strengthens the propensity of trustees to both delegate tasks to the organisation (β=0.875, p<0.0001) and to develop an increased intention to trust (β=0.971, p<0.0001) the target organisation. The amplifying effect of information security controls on reputation thus helps to improve the willingness of trustors to be vulnerable through delegating tasks and two-way communication. This finding has implications in terms of the interpretation of InfoSec controls for the Theory of Planned Behaviour.

An additional finding from the experimental results is that there is a positive covariance (β= 0.698) between Communication Quality and Outcomes. Outcomes was proposed as a research construct as the conjunction of both Delegation and Communication Quality. However, no empirical evidence was found that outcomes arise as a result of delegated action (β=0.187, p=0.081) and the hypothesis H6 was rejected. Therefore, it was shown that outcomes do not appear directly as a result of Delegation of tasks. Outcomes represent the meaning of joint behaviours that arise as a result of the presence of trust in the relationship, regardless of the amount of delegated tasks, and therefore power, that the trustee performs. This finding has implications for Social Exchange Theory, by helping to differentiate 'currencies' of exchange, with both economic and social benefits appearing as a result of joint action, but these may not necessarily be directly related.

It was an unexpected finding that there was no direct relationship between the outputs of delegation to the trustee and the consequent outcomes. That there is no relationship between delegation and outcomes seems unlikely as this would imply that blanket trust was in effect. It can be asserted that delegation is not therefore necessary for outcomes, and that there may be a connecting variable missing from the model. Sirdeshmukh et al. (2002)

investigated the role of value in trust relationship outcomes, and further research into the behavioural aspects of trust in the realisation of the value of delegated outputs in shaping outcomes is recommended.

A full listing of the model hypothesis testing is shown in Table 9.1 , and the implications of the research findings are discussed in Section 9.4.

Table 9.1 Hypothesis Testing Summary

Path	**Hypothesis**	**β**	***p*-value**
Information Security → Reputation	H1	0.853	p<0.0001
Reputation → Trust	H2	0.971	p<0.0001
Trust → Communication Quality	H3	0.944	p<0.0001
Reputation → Delegation	H4	0.875	p<0.0001
Communication Quality → Outcomes	H5	0.698	p<0.0001
Delegation → Outcomes	H6	0.187	p = 0.081

9.2 Research Aims

The investigation was directed by the four major research questions that were posed in the introduction, and the research effort was directed towards investigation of the links between cybersecurity and trust formation by posing the question:

- To what extent and how does information security influence and inform trust online?

This question was answered fully by the research, which revealed that information security has a strong positive covariance with reputation ($\beta=0.843$, $p<0.0001$). The effects of security measures correlate significantly with those of reputation. Reputation in turn, has a strong positive correlation with trust ($\beta=0.974$, $p<0.0001$), and mediation analysis showed that reputation is a key mediator of the relationship between security and trust. The formation of trust also showed a strong covariance with communication quality ($\beta=0.887$, $p<0.0001$) and was also shown by mediation analysis to be a key mediator of the relationship between reputation and communication quality.

Information security strongly influences reputation, which in turn strongly influences the formation of trust between parties. One of the outcomes of this trust formation is an improvement of communication quality between exchange partners. The effect is reasoned as communicating the values of the organisation and appreciating the importance of security to potential trustors realises the formation of trust via the mechanism of salient value congruence (Siegriest et al., 2000), displaying that it is safe to trust.

The second aim of the research was related to the interplay of trust and behaviour, and was framed as:

- What is the importance and role of trust in behaviour in digital environments?

This question was answered by examining the behavioural consequences of action, the outcomes. Outcomes allow a leeway of forgiveness in actions that have indelible consequences, and this was shown to be one of the hallmarks of the presence of trust in the

research findings. The quality of communication found in responses where trust was present were instrumental in achieving outcomes for the trusting party ($\beta=0.704$, $p<0.0001$). It was shown that Delegation is an operation that happens regardless of trusting intention, and was shown not to be directly related to behavioural outcomes ($\beta=0.187$, $p=0.081$). This research has, therefore managed to isolate a behavioural characteristic that is unique to trusting relationships.

The logical implication of the findings on the question of the importance and role of trust on behaviour online is, therefore, unrelated to task delegation to the organisation. The role of trust is in enabling outcomes that would not be achievable via delegation alone. This strongly suggests that, even in electronic environments, trust is important in binding trustors and trustees in shared outcomes and endeavours, beyond the transactional. The emergent role of trust is to enable the communication that allows for the interpretation of situations where neither side has an information advantage. Trust plays a role in allowing trustors to disclose vulnerability information to seek the social benefits of association, whilst allowing trustees both to meet and manage the confident expectations of these trustees whilst retaining the rewards of the customer association and the support of their peer organisations.

Electronic interaction is an area that enables communication in different scenarios, and the research chose to focus on how these affect the relationships between the constructs and was posed as:

- Do contexts moderate the role and effects of information security on trusting behaviour?

This question was answered using the scenario contexts to establish the stability of the research model and to give insight into the relative differences in the constructs between domain sub models. The research found measurement invariance that demonstrated that the constructs were consistent across the scenarios chosen. The model was tested and found to be stable across the contexts. Differences in the covariance between domain models was found and the statistics were used to infer the management contributions detailed in Section 9.5.

An answer to the fourth question was sought, not through direct means, but by a process of reflective inference based upon the answers to the first three questions. It was outlined as:

- What is the role of information security in the formation of trust in socio-technical environments?

It is clear from the research that information security controls are a component of reputation, which is a key influencer in the formation of trust and the consequent behavioural outcomes. These benefits are felt in all of the scenarios examined in the research. The definition of security as representing safety and freedom from threat extends the security guarantees offered in the environment offered by institutional protocols and contributes to the sense of care and belongingness felt by trustors (Maslow, 1943).

The role of information security from an organisational perspective allows a degree of control over the actions of trustors, and conversely, a degree of latitude in action for trustees. Security of information passed between the parties ensures that the details of vulnerabilities

that the trustor may not want to make public are shielded from view. This allows the information exchange necessary to investigate and resolve complex situations. Information Security online mimics the codes of secrecy and privacy enshrined in medical and banking environments that allow trustors to seek advice from trustees that are concerned about the welfare of them as individuals. This, in turn, cements the reputation of the trustee as a tactful listener in deciding the best course of action for the individual. The researchers' reflections on the findings and their insights into the role of security in trust formation are detailed in Section 9.7.4.

9.3 Research Objectives

The work undertaken to address these questions were formulated to direct the research effort, and the outcomes from these objectives are detailed in the following points:

- To conduct a comprehensive review of the literature as it relates to trust and information security. The literature relating to the problem area was critically reviewed and evaluated in **Chapter 2** of this thesis. This was used as a baseline from which the model and research hypotheses were drawn.
- To develop a definition of information security as it relates to trust. The meta-analysis and working definition of trust for the purposes of this thesis is included in **Section 2.3.**
- To develop a conceptual model of information security and trust formation, with the aim of making theoretical contribution by further developing the areas of theory

underpinning the research work. This objective was met and is included in **Section 3.2.1.**

- To produce an integrated logical model of information security and trust that was tested using scaled data collected from the UK general public. This objective was met and is included in **Section 3.2.8.**
- To define contexts of cybersecurity concern with which to statistically test the stability and generalisability of the logical research model. This objective was met and is included in **Section 3.2.9.**

Meeting and fulfilling the objectives of this thesis allowed the generation of models that were tested using descriptive and multidimensional statistical techniques with which the research hypotheses were validated and accepted. Discussion of the hypotheses testing is analysed in the next sub section.

9.4 Thesis Contributions

This thesis has made theoretical contributions to knowledge in several areas of trust and information security research. It has extended existing theories on trust to include security variables with which to explain the presence of cybersecurity concerns online, an addition to the existing theories on trust formation. It has also contributed specific empirical evidence into the literature on the relationships between Information Security and Reputation, and Communication quality and outcomes. These contributions are included in the next sub sections.

9.4.1 Theoretical Contribution

The research informs the development of theory in trust to include an appreciation of the role of information security in the development and maintenance of reputation and trust. The research findings showed the mediation relationship that reputation plays in both delegation of tasks and in the formation of trust. Trust, in turn, promotes improved communication quality that enhances behavioural outcomes. Information security has a strong positive covariance relationship with reputation. As both information security policy and reputation are exogenous variables, they represent ways that organisations can demonstrate their trustworthiness credentials to potential customers.

The findings of the research represent a contribution to the Theory of Planned Behaviour through the introduction of information security as an environmental variable that influences the perceived behavioural control of individuals in the electronic environment. This is achieved by augmenting the reputation of the trustee organisation. The mechanism of reputation signalling is processed by the individual and influences the 'intention to trust'. The enhanced weighting of the perceived control provided by reputation allows the trustor to psychologically weigh the control they have over the situation in hand with their attitude and social norms.

As information security deals with information handling by emphasising the use of information in line with the norms and values of individuals, it influences both delegation behaviour and trust formation behaviours through reputation. Trust formation is more likely in either highly regulated or risky activities (Gefen and Pavlou, 2006), for example Healthcare

or Relationship Banking, which leads to outcomes that are not necessarily related to the outputs of the intermediary information systems. Delegated behaviour is more likely to be enacted where activities can be more closely monitored, for example, Retail or Transactional Banking scenarios, and success or failure can be more directly attributed to the enabling information systems.

The model affords an explanation of the role of trust that extends Social Exchange Theory via the finding that the delegation of tasks is not directly related to the provision of outcomes as a result of the association between parties. The information quality that exists between trusted parties runs separately from the transactions that bind them, Social Exchange Theory is based on the concept of delayed reciprocation that benefits both parties to exchange. Social obligation that cannot be enforced by contract is the driver of behaviour in socio-economic systems. Failure to discharge these obligations has consequences that are disadvantageous for the recipient of such services, be they an individual or an organisation (Blau, 1964:95).

The extension of Social Exchange Theory into the digital realm requires that trusting individuals give the gift of data in exchange for the assistance of organisations. Individuals who withhold information in the chosen scenarios of Healthcare, Banking, and Retail fail to be the recipients of assistance that depends upon the sharing of vulnerability. Likewise, the trustee organisations that collect and analyse the details of the vulnerabilities of others risk a normative backlash from other peer organisations for their indiscretion.

The norm of reciprocity applies to both the economic and the social aspects of exchange. Organisations with a robust information security stance will reap the benefits of

economic exchange, but also the extrinsic benefits of the association, independent of the supplier of the commodity. That is, the extrinsic benefits of advice, word of mouth recommendation, assistance and compliance that come as part of the association are related to the higher communication quality that comes with trust. This produces a positive feedback loop of reputation enhancement that is used as currency in future associations.

Greater information security affords organisations a way to enhance reputation. Reputation, in turn, elicits greater interaction with trustors, both for task delegation and trust formation. These characteristics form the two major outputs from information security measures that become investments and differentiators in modern socio-technical systems.

9.4.2 Information Security and Reputation

The research contributed to the theoretical development of trust by demonstrating strong empirical evidence that a positive covariance relationship exists between information security and reputation (β=0.853). Attestation of information security principles by organisations shows strong positive covariance in the perceived reputation effects of those organisations. Further mediation analysis showed that reputation fully mediated the relationship between information security and the delegation of tasks, an important finding that investment in displaying Information Security values is directly reflected in increased reputation, and therefore, propensity to delegate tasks to the trustee organisation.

Moderation effects were observed in the findings applied to the Information Security → Reputation → Delegation relationship when examined using the cyber awareness and privacy sensitivity attitudes reported by respondents. It was found that for both attitudes that

there was a significant positive effect on the first part of the relationship, from Information Security to Reputation seen for high and low cyber awareness, and high and low sensitivity. This effect was reduced in the second part of the relationship, from Reputation to Delegation. There was a negligible indirect effect from Information Security to Delegation. These results confirm the finding that Information Security is strongly linked to Reputation, but the effect did not find evidence of individuals relying solely on Information Security measures to delegate tasks.

9.4.3 Communication Quality and Outcomes

A secondary finding from the research enquiry was that Communication Quality (the bi-directional communication between parties) has a positive covariance relationship with the outcomes of delegated actions (β=0.698). Prior investigations into what makes trust a positive mediator in outcomes assessed the added value that was gained from the relationship (Sirdeshmukh et al., 2002). The finding from this research is important because it gives an insight into the mechanisms in play when delegated action, trusted or untrusted, result in system outputs that were not quite as expected. In these cases, trust plays a major mediating role in translating reputation into better communication, and therefore, improved outcomes.

The contextual findings provided evidence that this enhanced communication is a premium in the areas of banking and healthcare where *"Cybersecurity is not just about protecting data; it is fundamental for maintaining the safety, privacy and trust of patients"* (Martin et al., 2017). Outcomes are interpreted outputs where trust is applied.

9.5 Management Contributions

The practical implication of the research is in reframing the role of information security in management. The research produced strong, significant evidence that the effects of information security are reflected in the effects these measures have on the reputation of a company. Reputation directly co-varies with the delegation of tasks to the organisation, and in the production of trust that enhances communication and outcomes.

Therefore, it is now possible to say that information security measures that were traditionally associated with loss prevention and expense to organisations have a positive investment purpose, which is to enhance the reputation of the organisation. A failure of information security is a failure of reputation and will significantly impact the willingness of consumers to delegate action to them, and will deteriorate the trust based communication quality that leads to outcomes for individuals. A comparative analysis of the results of these contextual differences was used to compare the relative strengths of the model relationships in the different environments, as *"Risk influences trust, but context influences the actions"* (Gambetta, 1988).

9.5.1 Retail Cybersecurity Management

In retail, stronger relationships are elicited by using information security to increase reputation, and then using reputation for successful task delegation. Outcomes are shaped by the outputs of the behaviour and systems rather than the quality of the communication between parties. Therefore, in retail environments consumers choose to delegate based on reputation, and this reputation is earned in part through a good information security stance.

Customers rate outcomes based on the result of how well the task was completed, which in turn, enhances the reputation of the retailer. The higher covariance observed for delegation than outcomes in retail suggests that management information security based on good supply chain and fulfilment strategy increase positive outcomes and enhance reputation.

9.5.2 Banking Cybersecurity Management

In the banking scenario, individuals were less willing to delegate tasks based only on the reputation of the organisation. This suggested that it is less likely for customers to give 'carte blanche' to their bank in organising their financial wellbeing. However, higher observed covariance between Communication Quality and Outcomes inferred that the two-way communication between banks and customers had higher priority in terms of producing outcomes. This points to the presence of trust in banking enhancing outcomes by the bi-directional exchange process of feedback that is more prominent in this sector than it is in retail.

The research findings suggest that the quality of communication of information security by banking organisations demonstrates a commitment to customer values and shared norms of information handling. This helps to produce a positive enhancement to the reputation of the organisation, for both transaction delegation and relationship development. In choosing to emphasise the congruence of values between the bank and the customer trusting relationships can be generated that enhance the outcomes for both parties.

9.5.3 Healthcare Cybersecurity Management

In healthcare, Communication Quality was much higher than in the other scenarios and this suggested the greater presence of trust in the relationship. In healthcare, the higher reputation of the provider is more likely to lead to delegated tasks being carried out. Therefore, it appears that the combination of high reputation scores and high trust scores enable both the handing over of tasks to the provider as well as contributing to the outcomes of those tasks.

It can be inferred that outcomes in healthcare scenarios are realised as a result of both high reputation (supported by Information security values), and high levels of trusting communication. This may be due, in part, to the longitudinal nature of the patient-medical practitioner relationship, although this was not investigated as part of the research enquiry.

9.6 Limitations of the Study

The research enquiry was directed by the research questions and objectives that were set in the introduction to this thesis. As such, it was necessary to limit certain aspects of the investigation to ensure that a focused analysis of the subject was fulfilled. The research design was used to scope the research, with the boundaries of the research both containing and constraining the applicability of the outputs. Thus, the study was limited in the following respects.

9.6.1 Generalisability

This study was limited by design to the UK general population as the respondents were drawn solely from panel members supplied by the data collection provider. The sample did not recruit outside of this area, so the results of the survey may be subject to social desirable reporting and may not be generalizable to other countries (Steenkamp, 2010). This non-generalisability of findings is due in part to possible differences in power distance and the social orientation of respondents. These features can act as moderators on the relationships that were found in the research model for respondents that do not have a UK centric orientation (Hofstede et al., 2011).

The study results have generalisability due to the measurement invariance obtained from the application of the research model to the chosen scenarios, namely Retail, Banking, and Healthcare. The rationale for choosing these areas is detailed in Section 3.2.9, and is based on areas of cybersecurity concern at the time the study was being designed. The areas chosen represent large areas of interaction, where respondents were given scenarios, but were able to apply their own attitudes and norms based on their experiences. Retail experiences vary greatly, banking online is generally a transactional activity, and healthcare secondary use also covers a wide area, from research to administration. In seeking to generalise across sectors the fine grained detail captured in very specific scenarios is lost. The choice of methodologies, in utilising large cohorts of questionnaire respondents likewise sacrifices some lower level insights as a result of the necessity to achieve sufficient response for analysis. The aggregated nature of the insights obtained could be strengthened or

complemented by performing structured interviews or using additional qualitative research methods to capture richer data with which to perform the analysis.

9.6.2 Longitudinal Results

The survey instrument was utilised in a cross-sectional capacity to obtain what was essentially a snapshot of respondent attitudes to the research questions at a point in time. Certain research questions cannot be answered using this type of approach. In this instance, the approach used would not be able to answer questions of attitude over longer periods of time, such as the relationship changes (**Section 9.5.3**) in healthcare scenarios, or the effect of new legislation, for example the GDPR, on attitudes to information security. Longitudinal survey data can be interpreted using the same techniques as single surveys (Kline, 2005) using a panel research model to allow a fuller assessment of the 'Who, Where and When' factors involved in theory development, detailed in Section 3.2.10 of this thesis.

9.6.3 Scale Development Limitations

The scale and item development processes related in Chapter 5 of this thesis described the research approach taken to developing the questionnaire. The process used a method in which the items utilised were progressively narrowed, through review processes by experts, card sorted popularity ratings by raters, and feedback from pilot questionnaire respondents. The resultant scales produced were analysed for reliability by use of Cronbach Alpha and CFA analysis methods. This resulted in increasingly difficult inclusion judgements having to be made by the researcher based on these analyses. Dropping items from scales, and in the instance of the confidentiality construct dropping the whole construct, ensured that the

questions analysed fed into the model to give the highest model fit values when SEM modelling was carried out.

Although this produces the strongest evidence on which to base the conclusions of the inferential statistics, the process of purification led to constructs that were very narrow in their definition. Allowing a wider margin of error on the measurement scales, and reducing the model fit would have allowed for wider inclusion of question responses, at the expense of some inferential power. It was reasoned that the production of stronger inferential conclusions would lead to better research outcomes, arguably at the expense of some breadth of coverage.

9.6.4 Researcher Bias

Is it truly possible to be free of bias about latent variables that are so embedded into the layers of life and the researchers' background without having an implicit attitude towards seeking to prove the veracity of concepts that have importance in everyday events? Likewise, is it possible to separate the qualitative viewpoints of colleagues and advisors from the views and opinions expressed to the researcher? (Chenail, 2011). Although the choice of an anonymous survey was selected to avoid knowing the personal embeddedness of individuals, and any personal conflicts of interest in the outcome were declared as part of the ethics approval, ultimately the analysis and interpretation of those results was a creative effort on the part of the author. Assumptions were challenged and confirmation bias measures were taken (**Section 5.2.6**) to guard as far as was possible against partiality.

9.7 Recommendations for Future Research.

To address the limitations on applicability outlined in the previous sub sections, it is recommended that future research effort in this area should concentrated on increasing the generalisability of the findings by distributing the survey in a global setting, and by continuing the research on a longitudinal basis to assess the variation of information security and reputation over time.

This section also looks at additional research angles that could be taken to extend the scope of the research and findings to cover confidentiality issues, and the relationship between these and the provision of security.

9.7.1 Confidentiality in Context

The contextual nature of information confidentiality is one area where the research path is not yet fully explored. As has been demonstrated in this research, information security when framed as the values of an organisation contributes to the reputation and delegation of tasks to a trustee. Confidentiality (or information privacy) is concerned with how the data collected (especially sensitive data) is processed after collection, so represents how those values are enacted in practice.

The growth in the quantity of data collected as a result of big data technologies has meant that the shift in the quantity of data collected requires an appreciation of how the privacy qualities of that data that are collected are subsequently utilised, interpreted and the inferences made about individuals, as well as how the data are interpreted by organisational

decision makers (Merendinho et al., 2019). Increased amounts of data reduce the need to hold personal data for the purposes of profiling and service provision as the algorithms that feed business technology models rely more on group attributes of intention and behaviours and the amounts of data collected merely ensure that all classes of consumers are represented.

The utilisation of data in context is a growing concern for many, and future research in this area could utilise the scale developed for this study, but which was discarded due to item loading issues detailed in Section 9.6.3. Initial review of the scale indicated that there were clear trends visible in the privacy preferences of older respondents. A study into the privacy personas of online users could answer fundamental questions about the nature of security and privacy. Security measures are frequently taken to elicit trust that is subsequently betrayed by the loss of privacy due to profiling. This points to the fact that security is relatively easy to implement, but the correct contextualisation of data is less straightforward.

9.7.2 Security and Privacy

Privacy is generally conceptualised as a subset of security (Cavoukian, 2009) and therefore stronger security naturally leads to stronger privacy protections. This behaviour was not observed in earlier revisions of the research model used in this thesis using both security and confidentiality constructs. The reasons why open systems may behave differently to closed systems may be related to the presence or fears about 'Big Data' and surveillance and these factors introduce other confounding variables that act on open systems online.

The observed differences may stem from the fact that the expectations of confidentiality have been compromised themselves by breaches of trust or system defences, putting personal data into the public realm. The non-public, non-transparent nature of personal data sharing between legitimate organisations may also play a role. However, without further research in these areas the understanding of how computing systems guard against privacy concerns is opaque at best.

9.7.3 Delegation and Outcomes

The rejected hypothesis from this research, that there is a relationship between task delegation and the perceived outcomes of delegation provided a finding that ran counter to the proposed model. It was thought that delegation, in leading to outputs would have a direct influence on the outcomes. The existence of a direct relationship was rejected and further research is required in this area of behavioural trust to define how successful or unsuccessful delegation affects the perception of the outcomes of the interaction.

Digital environments, and research into Multi-Agent systems treat delegation of tasks and trust as synonymous variables. Delegating a task to an automated agent is assumed to be an act that depends upon reliance of output. As such systems extend into the realm of AI and prescriptive task execution, the chances for parties to exercise the communication quality that is the hallmark of trust become less common. Knowing and understanding the boundaries between outputs and outcomes extends this research into Human Computer Interaction in those contexts that are traditionally driven by the communication between practitioner and client.

9.7.4 Qualitative Research Directions

The irony of conducting a quantitative study into the nature of the qualitatively human trait of trust formation is not lost on the researcher. This study has successfully delivered on a research programme that has shed new insight into the role of security controls in trust formation in three areas of human endeavour.

It is natural to ask further questions of the research data in terms of the meaning that information security measures have on individuals. The chosen scenarios have left room with which to pursue a qualitative research path that adds meaning to the understanding of how information security and reputation elicit trust, and how the negotiation of communication improves outcomes. The validity of this research will come from the combined insights afforded by both research approaches. This would be of particular use in the areas like healthcare and relationship banking where systems are still socio-technical in nature.

9.8 Reflections and Thoughts

Returning to the observation made in the introduction to this thesis on why the notion of security is, or appears to be, merely a feature of the online domain, not mentioned in the prior literature. Security in psychological terms represents the protection of perceived control in conditions of risk. Security increases the tendency of individuals to take action, either using trust or not. Information security online is analogous with the tact, discretion and benevolence afforded by the trustee (Rousseau et al., 1998; Baier, 1986). This attribute is

alluded to in the literature, but not fully developed because in the real world normative punishments for such behaviour are more strongly enforced. The production of reputation through improved information security commitments is the electronic equivalent of the exercise of such diplomacy, and reflects the motivation of the trustee organisation to adhere to the normative constraints this brings. These normative forces are brought into play as a result of the signalling behaviour of the trustee, with other

Improving information security assurances may not necessarily bring the benefits of trust as it may prompt consumers to take a protected transaction approach, but will increase the amount of delegation opportunities afforded, with the trusted and non-trusted proportions of these types of transactions varying according to the context. Thus, the protection of consumers becomes a double edged sword for providers who rely on trust, as security decreases the latitude for trustees to propose different problem resolutions to consumers and consumers become more guarded in their actions towards trustees.

9.9 Discussion Chapter Conclusion

This enquiry took a structured research pathway towards answering the questions posed in the introduction about the role of information security in the formation of trust in socio-technical environments; How information security influences and inform trust online; What the importance and role of trust is in behaviour in digital environments; and whether context moderates the role and effects of information security on trusting behaviour.

These questions have been investigated and the research has produced answers to many of the areas of interest. These findings and their interpretation have been included in

this chapter. Contributions to the canon of theoretical work include an extension of the Theory of Planned Behaviour to include an appreciation of Information Security as part of the perception of behavioural control, and additional insight into the operation of delayed reciprocation and normative control in the Social Exchange Theory. These important contributions place information security measures as an essential part of a trustworthy online presence, which have implications for the management of cybersecurity in the scenarios explored.

Contributions to the management of cybersecurity and trust have been evidenced, and the differing results obtained for the three scenarios have produced insights specific to those domains. In online retail scenarios, where reputation is a precursor to purchase delegation, trustworthy information security practices in supply chain and fulfilment partners is a key element of trust formation. In banking scenarios, signalling information security demonstrates value congruence and so enhances the reputation of the organisation. This reputation uplift increases both the task delegation and trust formation aspects of the trustee-trustor relationship.

The boundaries of the findings were evaluated alongside the limitations of the study to aid the interpretation and application of the findings to the theoretical and management contributions. In undertaking a critical analysis of the implications of the study further research avenues in the areas of confidentiality, privacy, outcomes and the enrichment of the findings through additional qualitative methods have emerged.

10. Conclusion

The confident expectation of trust, a cornerstone of the organisation of human behaviour, represents a requirement for moving beyond survival and basic necessity towards the satisfaction of deeper needs (Maslow, 1943). These psychological needs of wholeness, justice, belongingness and truth allow individuals to mature through their relationships with others, allowing them to exercise agency through dependable relationships with the institutions with whom they interact.

As information and data on individuals is increasingly hoarded by these organisations, the societal implications for breach of trust in a global interconnected world are unpredictable and related. These implications require further work on understanding how to protect the conditions under which trust can operate. Academic work in the field of information systems that has traditionally concentrated on the algorithmic protection of transactions must now turn towards the human-centric management discipline to effectively balance and manage the protection of trust relationships in the dynamic systems of social and digital interaction that characterise modernity.

Organisations that elicit and create situations where trust is required must learn that information security is necessary but not sufficient in isolation to the formation and maintenance of healthy trust relationships. Attestations to information security principles play a part in reassuring trustors' safety, but these statements need to be backed up with effective communication, discretion and judicious sharing of information to preserve the benefits that grow from the fragile roots of trust.

References

ABC (2016) [online] Australian Blood Data Breach. https://www.abc.net.au/news/2016-10-28/red-cross-blood-service-admits-to-data-breach/7974036 . [15th June 2019].

Abdul-Rahman, A. and Hailes, S. (2000) January 'Supporting trust in virtual communities'. In *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences* IEEE, 1- 9.

Aggarwal, P. and Mazumdar, T. (2008) 'Decision delegation: A conceptualization and empirical investigation'. *Psychology & Marketing 25*(1), 71-93.

Ahituv, N., Igbaria, M. and Sella, A.V. (1998) 'The effects of time pressure and completeness of information on decision making'. *Journal of management information systems 15*(2), 153-172.

Ajzen, I. and Fishbein, M. (1975) *Belief, attitude, intention and behaviour: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Ajzen, I. and Fishbein, M. (1980) *Understanding attitudes and predicting social behaviour.* Englewood Cliffs, NJ: Prentice Hall.

Ajzen, I. (1985) 'From Intentions to Actions: A Theory of Planned Behaviour'. In *Action Control*. Berlin Heidelberg: Springer, 11-39.

Ajzen, I. (1991) 'The Theory of Planned Behaviour'. *Organizational Behaviour and Human Decision Processes 50*(2), 179-211.

Ajzen, I. (2005) *Attitudes, Personality, and Behaviour*. London: McGraw-Hill Education (UK).

Altman, I. and Taylor, D.A. (1973) *Social Penetration: The Development of Interpersonal Relationships*. Oxford, England: Holt, Rinehart & Winston.

Amit, R. and Schoemaker, P.J. (1993) 'Strategic Assets and Organizational Rent'. *Strategic Management Journal 14*(1), 33-46.

Anderson, A.R. and Jack, S.L. (2002) 'The Articulation of Social Capital in Entrepreneurial Networks: a glue or a lubricant?' *Entrepreneurship & Regional Development 14*(3), 193-210.

Anderson, C.L. and Agarwal, R. (2010) 'Practicing safe computing: a multimedia empirical examination of home computer user security behavioural intentions'. *MIS quarterly 34*(3), 613-643.

Anderson, J.C. and Gerbing, D.W. (1988) 'Structural equation modelling in practice: A review and recommended two-step approach'. *Psychological bulletin 103*(3), 411-423.

Anderson, J.C. and Narus, J.A. (1990) 'A model of distributor firm and manufacturer firm working partnerships'. *The Journal of Marketing* 54(1), 42-58.

Anderson, J.M. (2003) 'Why we need a new definition of information security'. *Computers & Security 22*(4), 308-313.

Anderson, N. and Schalk, R. (1998) 'The psychological contract in retrospect and prospect'. *Journal of organizational behaviour* 19, 637-647.

Archer, M. (1998) 'Introduction: Realism in the Social Sciences.' *Critical Realism: Essential Readings*, London: Routledge, 189-205.

Archer, M., Bhaskar, R., Collier, A., Lawson, T. and Norrie, A. (2013) '*Critical realism: Essential Readings'*. London: Routledge.

Arendt, H. ([1958], 2013) *The Human Condition*. University of Chicago Press.

Argyle, M. and Little, B.R. (1972) 'Do Personality Traits Apply to Social Behaviour?' *Journal for the Theory of Social Behaviour 2*(1), 1-33.

Ashby, W.R. and Goldstein, J. ([1968], 2011) Variety, Constraint, and the Law of Requisite Variety. *Emergence: Complexity and Organization 13*(1/2), 190-207

Aula, P. (2010) 'Social Media, Reputation Risk and Ambient Publicity Management'. *Strategy & Leadership 38*(6), 43-49.

Axelrod, R. (1986) 'An Evolutionary Approach to Norms'. *American Political Science Review 80*(04), 1095-1111.

Bagozzi, R.P., Yi, Y. and Phillips, L.W. (1991) 'Assessing Construct Validity in Organizational Research'. *Administrative Science Quarterly* 36(3), 421-458.

Baier, A. (1986) 'Trust and antitrust' *Ethics 96*(2), 231-260.

Ball, D., Simões Coelho, P. and Machás, A. (2004) 'The Role of Communication and Trust in explaining Customer Loyalty: An extension to the ECSI model'. *European Journal of Marketing 38*(9/10), 1272-1293.

Bandura, A., Adams, N.E., Hardy, A.B. and Howells, G.N. (1980) 'Tests of the Generality of Self-efficacy Theory'. *Cognitive therapy and research 4*(1), 39-66.

Barbalet, J. (2009) 'A Characterization of Trust, and its' Consequences'. *Theory and society 38*(4), 367-382.

Barber, B. (1983) .*The logic and limits of trust* (Vol. 96). New Brunswick, NJ: Rutgers University Press.

Barnett, J.H. and Karson, M.J. (1987) 'Personal Values and Business Decisions: An Exploratory Investigation'. *Journal of Business Ethics 6*(5), 371-382.

Barney, J.B. and Hansen, M.H. (1994) 'Trustworthiness as a Source of Competitive Advantage'. *Strategic management journal 15*(S1), 175-190.

Baron, R.M. and Kenny, D.A. (1986) 'the Moderator–Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations'. *Journal of personality and social psychology 51*(6), 1173.

Barth, A., Datta, A., Mitchell, J.C. and Nissenbaum, H. (2006) May. 'Privacy and Contextual Integrity: Framework and Applications'. In *Security and Privacy, 2006 IEEE Symposium on Security and Privacy (S&P'06)*. IEEE, 15.

Bateson, G. (1970) 'Form, Substance and Difference'. In *Essential Readings in Biosemiotics*, ed. D. Faveureau, London: Springer,501.

BBC [1] (2019) TSB Data Breach [online] https://www.bbc.co.uk/news/business-47085474. [15th July 2019].

BBC [2] (2019) TalkTalk Data Breach [online] https://www.bbc.co.uk/news/business-48351900 . [15th July 2019].

BBC (2018) British Airways Data Breach [online] https://www.bbc.co.uk/news/technology-45481976 . [15th July 2019].

Becher, T. (1989) *Academic Tribes and Territories: Intellectual Enquiry and the Cultures of Disciplines* (Milton Keynes, England: Society for Research into Higher Education/Open University Press). *Open University Press.*

Bentler, P.M. and Chou, C.P. (1987) 'Practical Issues in Structural Modelling'. *Sociological Methods & Research 16*(1), 78-117.

Bentler, P.M. (1990) 'Comparative Fit Indexes in Structural Models'. *Psychological Bulletin 107*(2), 238-246.

Berg, J., Dickhaut, J. and McCabe, K. (1995) 'Trust, Reciprocity, and Social History'. *Games and Economic Behaviour 10*(1), 122-142.

Berger, J. and Heath, C. (2007) 'Where Consumers Diverge from Others: Identity Signaling and Product Domains'. *Journal of Consumer Research 34*(2), 121-134.

Berthon, P.R., Pitt, L.F., McCarthy, I. and Kates, S.M (2007). 'When Customers get clever: Managerial Approaches to Dealing with Creative Consumers'. *Business Horizons 50*(1), 39-47.

Bestor, T.W. (1988) 'Plato's phaedo and Plato's 'essentialism''. *Australasian Journal of Philosophy 66*(1), 26-51.

Bhaskar, R. (2014) *The Possibility of Naturalism: A Philosophical Critique of the Contemporary Human Sciences'*. London: Routledge.

Bies, R.J. and Tripp, T. (1996) Beyond Distrust: 'Getting even' and the need for revenge'. In. R. Kramer, & T. Tyler (Eds.) *Trust in Organizations*, Thousand Oaks, CA: Sage, 246-260.

Blau, P.M. (1964) *Exchange and power in social life*. Transaction Publishers, NY: John Wiley & Sons.

Blois, K.J. (1999) 'Trust in Business to Business Relationships: An Evaluation of its' Status'. *Journal of Management Studies 36*(2), 197-215.

Blumer, H. (1986). *Symbolic Interactionism: Perspective and Method*. University of California Press.

Boeschoten, L., Oberski, D.L., De Waal, T. and Vermunt, J.K. (2018) 'Updating Latent Class Imputations with External Auxiliary Variables'. *Structural Equation Modelling: A Multidisciplinary Journal 25*(5), 750-761.

Bogdan, R. and Biklen, S. (1998) Introduction to Qualitative Research in Education. *England: Pearson*.

Bohnet, I., Herrmann, B. and Zeckhauser, R. (2010) 'Trust and the Reference Points for Trustworthiness in Gulf and Western countries'. *The Quarterly Journal of Economics 125*(2), 811-828.

Bollen, K.A. (1986) 'Sample size and Bentler and Bonett's non-normed fit index'. *Psychometrika 51*(3), 375-377.

Bollen, K.A. (1989) 'A New Incremental Fit Index for general Structural Equation Models'. *Sociological Methods & Research 17*(3), 303-316.

Bollen, K.A. (1990) 'Overall fit in covariance structure models: Two types of sample size effects'. *Psychological Bulletin*, *107*(2), 256-259.

Bowlby, J. ([1979], 2012) *The Making and Breaking of Affectional Bonds*. Routledge.

Bradach, Jeffrey L., and Robert G. Eccles (1989) 'Price, Authority, and Trust: From ideal types to plural forms.' *Annual Review of Sociology* 15(1), 97-118.

BRC (2019) British Retail Crime Survey [online]. https://brc.org.uk/media/404253/brc-annual-crime-survey-2019.pdf [15th June 2019].

Brown, T.A. and Moore, M.T. (2012) Confirmatory Factor Analysis. In *Handbook of Structural Equation Modelling* ed. by Hoyle, R.H. Guilford Press, 361-379.

Browne, M.W. and Cudeck, R. (1993) 'Alternative ways of assessing model fit'. *Sage Focus editions 154*, 136-136.

Burrell, G. and Morgan, G. (2017) *Sociological Paradigms and Organisational Analysis: Elements of the Sociology of Corporate Life*. Oxford: Routledge.

Byrne, B.M. (2016) *Structural Equation Modelling with AMOS: Basic concepts, applications, and programming*. Oxford: Routledge.

Caldwell, C. and Clapham, S.E. (2003) 'Organizational Trustworthiness: An International Perspective'. *Journal of Business Ethics 47*(4), 349-364.

Carrigan, M. and Attalla, A. (2001) 'The myth of the ethical consumer–do ethics matter in purchase behaviour?' *Journal of Consumer Marketing 18*(7), 560-578.

Casaló, L.V., Flavián, C. and Guinalíu, M. (2007) 'The Role of Security, Privacy, Usability and Reputation in the development of online banking'. *Online Information Review 31*(5), 583-603.

Castelfranchi, C. and Falcone, R. (1998) 'Towards a theory of delegation for agent-based systems'. *Robotics and Autonomous Systems 24*(3-4), 141-157.

Castelfranchi, C. and Falcone, R. (2005) *Socio-cognitive theory of trust*. J. Pitt. London: Wiley.

Castelfranchi, C., Falcone, R. and Marzo, F. (2006) May. 'Being trusted in a social network: Trust as relational capital'. In *International Conference on Trust Management*. Berlin, Heidelberg: Springer, 19-32.

Castells, M. and Castells, M. (1998) 'The Rise of the Network Society', the information age: economy, society and culture. Volume 1. The rise of the network society. *Environment and Planning B: Planning and Design 25*, 631-636.

Castells, M. (2005) 'Space of flows, space of places: Materials for a theory of urbanism in the information age'. In *Comparative Planning Cultures ed. by Sanyal, B*. Oxford: Routledge, 69-88.

Cavoukian, A. (2009) 'Privacy by Design: The 7 foundational principles'. *Information and Privacy Commissioner of Ontario, Canada*, *5*.

Chami, R. and Fullenkamp, C. (2002) 'Trust and Efficiency'. *Journal of Banking & Finance 26*(9), 1785-1809.

Chanley, V.A., Rudolph, T.J. and Rahn, W.M. (2000) 'The Origins and Consequences of Public Trust in Government: A time series analysis' *Public Opinion Quarterly 64*(3), 239-256.

Chen, I.J. and Popovich, K. (2003) 'Understanding Customer Relationship Management (CRM) People, process and technology'. *Business Process Management Journal 9*(5), 672-688.

Chen, K. and Rea Jr, A.I. (2004) 'Protecting Personal Information online: A survey of user privacy concerns and control techniques'. *Journal of Computer Information Systems 44*(4), 85-92.

Chen, P.Y. and Hitt, L.M. (2002) 'Measuring switching costs and the determinants of customer retention in Internet-enabled businesses: A study of the online brokerage industry'. *Information Systems Research 13*(3), 255-274.

Chenail, R.J. (2011) 'Interviewing the Investigator: Strategies for addressing instrumentation and researcher bias concerns in qualitative research'. *The Qualitative Report 16*(1), 255-262.

Chiles, T.H. and McMackin, J.F. (1996) 'Integrating variable risk preferences, trust, and transaction cost economics'. *Academy of Management Review 21*(1), 73-99.

Choucri, N., Madnick, S. and Ferwerda, J. (2014) 'Institutions for Cyber Security: International responses and global imperatives'. *Information Technology for Development 20*(2), 96-121.

Churchill Jr, G.A. (1979) 'A paradigm for developing better measures of marketing constructs'. *Journal of Marketing Research 16*(1), 64-73.

Clague, C., Keefer, P., Knack, S. and Olson, M. (1996) 'Property and contract rights in autocracies and democracies'. *Journal of Economic Growth 1*(2), 243-276.

D. D. Clark, D. R. Wilson (1987) 'A comparison of commercial and military computer security policies', *Security and Privacy 1987 IEEE Symposium*, April 1987, 184-187.

Cohen, J. (2001) 'Defining identification: A theoretical look at the identification of audiences with media characters'. *Mass Communication & Society 4*(3), 245-264.

Coleman, J.S. (1988) 'Social capital in the creation of human capital'. *American Journal of Sociology 94*, S95-S120.

Colquitt, J.A. and Rodell, J.B. (2011) 'Justice, Trust, and Trustworthiness: A longitudinal analysis integrating three theoretical perspectives'. *Academy of Management Journal 54*(6), 1183-1206.

Coltman, T., Devinney, T.M., Midgley, D.F. and Venaik, S. (2008) 'Formative versus Reflective measurement models: Two applications of formative measurement'. *Journal of Business Research 61*(12), 1250-1262.

Comte, A. (1975) *Auguste Comte and Positivism: The essential writings* ed. by Lenzer, G. Transaction Publishers.

Connelly, B.L., Certo, S.T., Ireland, R.D. and Reutzel, C.R. (2011) 'Signaling theory: A review and assessment'. *Journal of Management 37*(1), 39-67.

Conte, R. and Castelfranchi, C. (2016) *Cognitive and social action*. Garland Science.

Cooper, R., DeJong, D.V., Forsythe, R. and Ross, T.W. (1992) 'Communication in coordination games'. *The Quarterly Journal of Economics 107*(2), 739-771.

Coppola, N.W., Hiltz, S.R. and Rotter, N.G. (2004) 'Building trust in virtual teams'. *IEEE Transactions on Professional Communication 47*(2), 95-104.

Corner, S. (2009) 'Choosing the right type of rotation in PCA and EFA'. *JALT testing & Evaluation SIG newsletter 13*(3), 20-25.

Coughlan, R. (2005) 'Employee Loyalty as Adherence to Shared Moral Values'. *Journal of Managerial Issues* 17(1), 43-57.

Cousineau, D., Brown, S. and Heathcote, A. (2004) 'Fitting Distributions using Maximum Likelihood: Methods and Packages'. *Behavior Research Methods, Instruments, & Computers 36*(4), 742-756.

Creswell, J.W. and Creswell, J.D. (2017) *Research Design: Qualitative, Quantitative, and Mixed Methods approaches*. Sage publications.

Cropanzano, Russell, and Marie S. Mitchell (2005) 'Social Exchange Theory: An interdisciplinary review.' *Journal of Management* 31(6), 874-900.

Crosby, L.A., Evans, K.R. and Cowles, D. (1990) 'Relationship Quality in Services Selling: An interpersonal influence perspective'. *The Journal of Marketing* 54(3), 68-81.

Cvetkovich, G., Siegrist, M., Murray, R. and Tragesser, S. (2002) 'New Information and Social Trust: Asymmetry and perseverance of attributions about hazard managers'. *Risk Analysis*, *22*(2), 359-367.

Darby, M.R. and Karni, E. (1973) 'Free competition and the optimal amount of fraud'. *The Journal of Law and Economics*, *16*(1), 67-88.

Das, T.K. (2006) 'Strategic Alliance Temporalities and Partner Opportunism'. *British Journal of Management*, *17*(1), 1-21.

Dasgupta, P. (2000) 'Trust as a Commodity'. In Gambetta, D. ed. *Trust: Making and breaking cooperative relations*. New York, NY: B. Blackwell, 49-72.

Davies, L. (2016) 'Security, Extremism and Education: Safeguarding or Surveillance?' *British Journal of Educational Studies 64*(1), 1-19.

Davis, F.D., Bagozzi, R.P. and Warshaw, P.R. (1989) 'User Acceptance of Computer Technology: a comparison of two theoretical models'. *Management Science 35*(8), 982-1003.

De Marneffe, M.C., Manning, C.D. and Potts, C. (2012) 'Did it happen? The Pragmatic Complexity of Veridicality Assessment'. *Computational Linguistics 38*(2), 301-333.

De Oliveira Albuquerque, R., Villalba, L.J.G., Orozco, A.L.S., de Sousa Júnior, R.T. and Kim, T.H. (2016) 'Leveraging Information Security and Computational Trust for Cybersecurity'. *The Journal of Supercomputing 72*(10), 3729-3763.

De Sousa, R. (1979) 'The Rationality of Emotions'. *Dialogue 18*(01), 41-63.

Derlega, V.J. and Chaikin, A.L. (1977) 'Privacy and self-disclosure in social relationships'. *Journal of Social Issues 33*(3), 102-115.

Deutsch, M. (1958) 'Trust and Suspicion'. *Journal of Conflict Resolution*, 265-279.

Devlin, K. (1995) *Logic and Information*. Cambridge University Press.

Devos, T., Spini, D. and Schwartz, S.H. (2002) 'Conflicts among Human Values and Trust in Institutions'. *British Journal of Social Psychology 41*(4), 481-494.

Dey, A.K. (2001) 'Understanding and using context'. *Personal and Ubiquitous Computing 5*(1), 4-7.

Diamantopoulos, A. (2005) 'The C-OAR-SE procedure for scale development in marketing: a comment'. *International Journal of Research in Marketing 22*(1), 1-9.

Diamantopoulos, A. and Winklhofer, H.M. (2001) 'Index construction with formative indicators: An alternative to scale development.' *Journal of Marketing Research*, *38*(2), pp.269-277.

Dibb, S. and Meadows, M. (2001) 'The Application of a Relationship Marketing Perspective in Retail Banking'. *Service Industries Journal 21*(1), 169-194.

Dietz, G. and Den Hartog, D.N. (2006) 'Measuring Trust inside Organisations'. *Personnel Review 35*(5), 557-588.

Dirks, K.T. (2000) 'Trust in leadership and team performance: evidence from NCAA basketball'. *Journal of Applied Psychology 85*(6), 1004-1012.

Disterer, G. (2013) ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security* 2013 (4), 92-100

Djupe, P.A. and Calfano, B.R. (2009) 'Justification not by faith alone: Clergy generating trust and certainty by revealing thought'. *Politics and Religion 2*(01), 1-30.

Doan, A., Domingos, P. and Halevy, A.Y. (2001) May. 'Reconciling schemas of disparate data sources: A machine-learning approach'. In ACM: *ACM Sigmod Record* 30(2), 509-520.

Dobson, P.J. (2002) 'Critical Realism and Information Systems Research: why bother with philosophy?' *Information Research, 7*(2).

Donath, J. (2007) 'Signals in Social Supernets'. *Journal of Computer-Mediated Communication 13*(1), 231-251.

Doney, P.M. and Cannon, J.P. (1997) 'An Examination of the nature of trust in buyer-seller relationships'. *The Journal of Marketing* 61(2), 35-51.

Douceur, J.R. (2002) March. The Sybil attack. In *International workshop on peer-to-peer systems* (pp. 251-260). Springer, Berlin, Heidelberg.

Duhan, D.F., Johnson, S.D., Wilcox, J.B. and Harrell, G.D. (1997) 'Influences on Consumer use of word-of-mouth recommendation sources'. *Journal of the Academy of Marketing Science 25*(4), 283-295.

Dunfee, T.W., Smith, N.C. and Ross Jr, W.T. (1999) 'Social Contracts and Marketing Ethics'. *Journal of Marketing 63*(3), 14-32.

Eastlick, M.A., Lotz, S.L. and Warrington, P. (2006) 'Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment'. *Journal of Business Research 59*(8), 877-886.

Eaton, J.J. and Bawden, D. (1991) 'What kind of resource is information?' *International Journal of Information Management 11*(2), 156-165.

Eccles, R.G. and White, H.C. (1988) 'Price and Authority in inter-profit Center transactions'. *American Journal of Sociology 94*, S17-S51.

Edwards, J.R. and Bagozzi, R.P. (2000) 'On the nature and direction of relationships between constructs and measures'. *Psychological Methods 5*(2), 155.

Edwards, J.R. and Lambert, L.S. (2007) 'Methods for integrating moderation and mediation: a general analytical framework using moderated path analysis.' *Psychological methods 12*(1), 1.

Einhorn, H.J. and Hogarth, R.M. (1981) Behavioral Decision Theory: Processes of judgement and choice'. *Annual Review of Psychology 32*(1), 53-88.

Eisenhardt, K.M. (1989) 'Agency Theory: An assessment and review'. *Academy of Management Review 14*(1), 57-74.

Elangovan, A.R. and Shapiro, D.L. (1998) 'Betrayal of trust in organizations'. *Academy of Management Review 23*(3), 547-566.

Elangovan, A.R., Auer-Rizzi, W. and Szabo, E. (2007) 'Why don't I trust you now? An attributional approach to erosion of trust'. *Journal of Managerial Psychology 22*(1), 4-24.

Enders, C.K. and Bandalos, D.L. (2001) 'The relative performance of full information maximum likelihood estimation for missing data in structural equation models'. *Structural equation modelling 8*(3), 430-457.

England.nhs.uk (2018) NHS GP Patient Survey [online] https://www.england.nhs.uk/statistics/2018/08/09/gp-patient-survey-2018/ .[15th June 2019].

Engler, T.H., Winter, P. and Schulz, M. (2015) 'Understanding online product ratings: A customer satisfaction model'. *Journal of Retailing and Consumer Services 27*, 113-120.

Erikson, E.H. (1965) *Childhood and Society. (Revised Edition)*. Penguin Books.

Evans, A.M. and Revelle, W. (2008) 'Survey and behavioural measurements of interpersonal trust'. *Journal of Research in Personality 42*(6), 1585-1593.

Eyal, I. and Sirer, E.G. (2014) March. 'Majority is not enough: Bitcoin mining is vulnerable'. In *International Conference on Financial Cryptography and Data Security 2014*. Berlin, Heidelberg: Springer, 436-454.

Falcone, R. and Castelfranchi, C., 2001. 'Social trust: A cognitive approach'. In Castelfranchi, C. and Tan, Y.H. eds., 2001. *Trust and Deception in Virtual Societies*. Dordrecht: Springer, 55-90.

Falcone, R. and Castelfranchi, C. (2008) May. 'Generalizing trust: Inferencing trustworthiness from categories'. In *International Workshop on Trust in Agent Societies*. Berlin, Heidelberg: Springer, 65-80.

Fehr, E. and Schmidt, K.M. (1999) 'A theory of fairness, competition, and cooperation'. *The Quarterly Journal of Economics 114*(3), 817-868.

FFAUK (2017) UK Payment Industry Fraud Overview, 2017. [online] https://www.financialfraudaction.org.uk/fraudfacts17/ . [15th June 2019].

Fischbacher, U., Gächter, S. and Fehr, E. (2001) 'Are people conditionally cooperative? Evidence from a public goods experiment'. *Economics Letters 71*(3), 397-404.

Fischer, F. (1998) 'Beyond Empiricism: policy inquiry in post positivist perspective'. *Policy Studies Journal 26*(1), 129-146.

Fishbein, M. and Ajzen, I. ([1975], 1977) *Belief, Attitude, and Behavior: An introduction to theory and research.* Reading, Mass.: Addison Wessley.

Fisman, R. and Khanna, T. (1999) 'Is trust a historical residue? Information flows and trust levels'. *Journal of Economic Behavior & Organization 38*(1), 79-92.

Flavián, C. and Guinalíu, M. (2006) Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site' *Industrial Management & Data Systems 106*(5), 601-620.

Flores, F. and Solomon, R.C. (1998) 'Creating Trust'. *Business Ethics Quarterly* 8(2), 205-232.

Floyd, F.J. and Widaman, K.F. (1995) 'Factor analysis in the development and refinement of clinical assessment instruments'. *Psychological Assessment 7*(3), 286.

Fornell, C. and Larcker, D.F. (1981) 'Evaluating structural equation models with unobservable variables and measurement error'. *Journal of Marketing Research 18*(1), 39-50.

Frankfort-Nachmias, C. and Nachmias, D. (2007) '*Study guide for research methods in the social sciences'*. London: Macmillan.

Frederick, S. (2005) 'Cognitive Reflection and Decision Making'. *The Journal of Economic Perspectives 19*(4), 25-42.

Fukuyama, F. (1995) *Trust: The social virtues and the creation of prosperity* (Vol. 99). New York, NY: Free Press.

Futter, A. (2018) ‘‘Cyber’semantics: why we should retire the latest buzzword in security studies’. *Journal of Cyber Policy 3*(2), 201-216.

Gambetta, D. (1988) ‘Trust: Making and breaking cooperative relations’. In Gambetta, D. ed., *Trust: Making and breaking cooperative relations*. New York, NY: B. Blackwell, 213-238.

Gambetta, Diego (2000) ‘Can We Trust Trust?’ In Gambetta, Diego (ed.) *Trust: Making and Breaking Cooperative Relations*, electronic edition, Department of Sociology, University of Oxford, chapter 13, 213-237.

Gefen, D. (2000) ‘E-commerce: the role of familiarity and trust’. *Omega 28*(6), 725-737.

Gefen, D., Benbasat, I. and Pavlou, P. (2008) ‘A research agenda for trust in online environments’. *Journal of Management Information Systems 24*(4), 275-286.

Gefen, D., Karahanna, E. and Straub, D.W. (2003) ‘Trust and TAM in online shopping: an integrated model’. *MIS Quarterly 27*(1), 51-90.

Gefen, D., Rao, V.S. and Tractinsky, N. (2003) ‘January. The conceptualization of trust, risk and their electronic commerce: the need for clarifications’. In *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on*. IEEE, 10

Gefen, D. and Pavlou, P.A. (2006) December. An inverted-U theory of trust: The moderating role of perceived regulatory effectiveness of online marketplaces. In *Twenty Seventh International Conference on Information Systems*.

Gefen, D., Rigdon, E.E. and Straub, D. (2011) ‘Editor's comments: an update and extension to SEM guidelines for administrative and social science research’. *MIS Quarterly*, iii-xiv.

Geldhof, G.J., Preacher, K.J. and Zyphur, M.J. (2014) ‘Reliability estimation in a multilevel confirmatory factor analysis framework’. *Psychological Methods 19*(1), 72.

Gerck, E. (2002) 'Trust as Qualified Reliance on information'. *The COOK Report on Internet, X (10)*, 19-24.

Gerck, E., Neff, C.A., Rivest, R.L., Rubin, A.D. and Yung, M. (2001) February. 'The business of electronic voting'. In *International Conference on Financial Cryptography* 2001. Berlin Heidelberg: Springer, 243-268.

Gheorghiu, M.A., Vignoles, V.L. and Smith, P.B. (2009) 'Beyond the United States and Japan: Testing Yamagishi's emancipation theory of trust across 31 nations'. *Social Psychology Quarterly 72*(4), 365-383.

Giddens, A. (1984) *The constitution of society: Outline of the theory of structuration*. University of California Press.

Giddens, A. (1991) *Modernity and self-identity: Self and society in the late modern age*. Stanford University Press.

Gigerenzer, G. and Selten, R. (2002) *Bounded Rationality: The adaptive toolbox*. MIT press.

Gliem, J.A. and Gliem, R.R. (2003) 'Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales'. Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education 2003.

Goffman, E., 1978. *The presentation of self in everyday life*. London: Harmondsworth.

Golbeck, J. and Hendler, J. (2006) 'Inferring binary trust relationships in web-based social networks'. *ACM Transactions on Internet Technology (TOIT) 6*(4), 497-529.

Goldsmith, J. and Junker, U. (2008) 'Preference handling for artificial intelligence'. *AI Magazine 29*(4), 9-17.

Gollwitzer, P.M. (1999) 'Implementation intentions: Strong effects of simple plans.' *American Psychologist 54*(7), 493.

Good, D. (2000) 'Individuals, interpersonal relations, and trust'. In Gambetta, D. ed., *Trust: Making and breaking cooperative relations*. New York, NY: B. Blackwell, 31-48.

Goodwin, C. (1991) 'Privacy: Recognition of a consumer right'. *Journal of Public Policy & Marketing* 10(1), 149-166.

Gotsi, M. and Wilson, A.M. (2001) 'Corporate reputation: seeking a definition'. *Corporate Communications: An International Journal 6*(1), 24-30.

Grandison, T. and Sloman, M. (2003) May. 'Trust management tools for internet applications'. In *International Conference on Trust Management 2003*. Berlin, Heidelberg: Springer, 91-107.

Granovetter, M. (1985) 'Economic Action and social structure: The problem of embeddedness'. *American Journal of Sociology 91*(3), 481-510.

Granovetter, M.S. (1973) 'The strength of weak ties'. *American Journal of Sociology 78*(6), 1360-1380.

Greenspan, P. (2000) 'Emotional strategies and rationality'. *Ethics 110*(3), 469-487.

Greenwald, G. (2014) *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. Macmillan.

Griffiths, N. (2005) July. 'Task delegation using experience-based multi-dimensional trust'. In *Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems*. ACM, 489-496.

Guba, E.G. and Lincoln, Y.S. (1994) 'Competing paradigms in qualitative research'. *Handbook of qualitative research*, *2*(no. 163-194), 105.

Guba, E.G. (1981) 'Criteria for assessing the trustworthiness of naturalistic inquiries'. *Educational Communication and Technology Journal 29*(2), 75.

Guba, E.G. (1990) 'The paradigm dialog'. In *Alternative Paradigms Conference, Mar, 1989, Indiana U, School of Education, San Francisco, CA, US*. Sage Publications, Inc.

Ha, H.Y. (2004) 'Factors influencing consumer perceptions of brand trust online'. *Journal of Product & Brand Management 13*(5), 329-342.

Habermas, J., 1984. *The theory of communicative action* (Vol. 2). Boston, MA: Beacon press.

Haig, B.D. (2008) 'An Abductive Perspective on Theory Construction'. *Journal of Theory Construction & Testing 12*(1), 7-10.

Hair, J.F., Anderson, R.E., Babin, B.J. and Black, W.C. (2010) Multivariate data analysis: A global perspective (Vol. 7). Upper Saddle River: Pearson.

Hallebone, E. and Priest, J. (2008) *Business and management research: paradigms and practices*. Macmillan International Higher Education.

Hancock, J.T., Toma, C. and Ellison, N. (2007) April. 'The truth about lying in online dating profiles' In *Proceedings of the SIGCHI conference on Human factors in computing systems* ACM. 449-452.

Hansen, J.M., Saridakis, G. and Benson, V. (2018) 'Risk, trust, and the interaction of perceived ease of use and behavioral control in predicting consumers' use of social media for transactions'. *Computers in Human Behavior 80*, 197-206.

Hardin, R. (1992) 'The street-level epistemology of trust'. *Analyse & Kritik 14*(2), 152-176.

Hardin, R. (1996) 'Trustworthiness'. *Ethics 107*(1), 26-42.

Hardin, R. (2002) *Trust and trustworthiness*. Russell Sage Foundation.

Hattie, J. (1985) 'Methodology review: assessing unidimensionality of tests and items'. *Applied Psychological Measurement 9*(2), 139-164.

Haug, A. and Stentoft Arlbjørn, J. (2011) 'Barriers to master data quality'. *Journal of Enterprise Information Management 24*(3), 288-303.

Hibberd, F.J. (2006) *Unfolding social constructionism*. Springer Science & Business Media.

Hill, K. (2012) How target figured out a teen girl was pregnant before her father did. *Forbes, Inc*. [online] https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/ [16th July 2019].

Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R. and Taylor, R. (2005) 'Can electronic medical record systems transform health care? Potential health benefits, savings, and costs'. *Health affairs 24*(5), 1103-1117.

Hobbes, T. ([1561], 2006). *Leviathan*. A&C Black.

Hoffman, D.L., Novak, T.P. and Peralta, M. (1999) 'Building consumer trust online'. *Communications of the ACM 42*(4), 80-85.

Hofstede, G. (1980) 'Culture and organizations'. *International Studies of Management & Organization 10*(4), 15-41.

Hofstede, G. (2011) 'Dimensionalizing cultures: The Hofstede model in context'. *Online Readings in Psychology and Culture 2*(1), 8.

Holton, R. (1994) 'Deciding to trust, coming to believe'. *Australasian Journal of Philosophy 72*(1), 63-76.

Hong, I.B. and Cho, H. (2011) 'The impact of consumer trust on attitudinal loyalty and purchase intentions in B2C e-marketplaces: Intermediary trust vs. seller trust'. *International Journal of Information Management 31*(5), 469-479.

Hosmer, L.T. (1995) 'Trust: The connecting link between organizational theory and philosophical ethics'. *Academy of Management Review 20*(2), 379-403.

Hu, L.T. and Bentler, P.M. (1998) 'Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification'. *Psychological Methods 3*(4), 424.

Hu, L.T. and Bentler, P.M. (1999) 'Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives'. *Structural Equation Modeling: a Multidisciplinary Journal 6*(1), 1-55.

Hu, L.T., Bentler, P.M. and Kano, Y. (1992) 'Can test statistics in covariance structure analysis be trusted?' *Psychological Bulletin 112*(2), 351.

Huang, M.H. and Chen, C.Y. (2016) July. 'Antecedents and Outcomes of Trust in Professional Associations'. In *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2016 10th International Conference.* IEEE, 541-545.

Huang, X., Xiang, Y., Bertino, E., Zhou, J. and Xu, L. (2014) Robust multi-factor authentication for fragile communications. *IEEE Transactions on Dependable and Secure Computing*, *11*(6), pp.568-581.

Hunt, S.D. (1991) 'Positivism and paradigm dominance in consumer research: toward critical pluralism and rapprochement'. *Journal of Consumer Research 18*(1), 32-44.

Hwang, Y. and Lee, K.C. (2012) 'Investigating the moderating role of uncertainty avoidance cultural values on multidimensional online trust'. *Information & Management 49*(3-4), 171-176.

Hyland, K. (1999) 'Academic attribution: Citation and the construction of disciplinary knowledge'. *Applied Linguistics 20*(3), 341-367.

Iacobucci, D. (2010) 'Structural equations modeling: Fit indices, sample size, and advanced topics'. *Journal of Consumer Psychology 20*(1), 90-98.

References

ICO [1] (2018) ICO Guidance on implementing the GDPR. [online] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ . [15th June 2019].

ICO [2] (2018) ICO Guidance on implementing encryption https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/what-is-encryption/ . [15th June 2019].

Im, I., Hong, S. and Kang, M.S. (2011) 'An International comparison of technology adoption: Testing the UTAUT model'. *Information & Management*, *48*(1), 1-8.

Jaccard, J., Wan, C.K. and Jaccard, J. (1996) *LISREL approaches to interaction effects in multiple regression* (No. 114). London: Sage.

Jakobsson, M. and Myers, S. eds. (2006) *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. John Wiley & Sons.

Jarvenpaa, S.L. and Leidner, D.E. (1999) 'Communication and trust in global virtual teams'. *Organization Science 10*(6), 791-815.

Jensen, M.C. and Meckling, W.H. (1976) 'Theory of the firm: Managerial behavior, agency costs and ownership structure'. *Journal of Financial Economics 3*(4), 305-360.

Jick, T.D. (1979) 'Mixing qualitative and quantitative methods: Triangulation in action'. *Administrative Science Quarterly 24*(4), 602-611.

Joachims, T. (2002) July. 'Optimizing search engines using clickthrough data.' In *Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM. 133-142.

Johnson, D. and Grayson, K. (2005) 'Cognitive and affective trust in service relationships'. *Journal of Business Research 58*(4), 500-507.

Johnson, D.S. and Grayson, K. (2000). *Sources and dimensions of trust in service relationships*. Thousand Oaks, CA: Sage, 357-370.

Joinson, A.N., Paine, C., Buchanan, T. and Reips, U.D. (2008) 'Measuring self-disclosure online: Blurring and non-response to sensitive items in web-based surveys'. *Computers in Human Behavior 24*(5), 2158-2171.

Jones, G.R. and George, J.M. (1998) 'The Experience and evolution of trust: Implications for cooperation and teamwork'. *Academy of Management Review 23*(3), 531-546.

Jonker, J. and Pennink, B. (2010). *The Essence of research methodology: A concise guide for master and PhD students in management science*. Springer Science & Business Media.

Jöreskog, K.G., Sörbom, D. and Lisrel, V.I. (1984) *Analysis of linear structural relationship by maximum likelihood.* Moorsville, IN: Scientific Software.

Jøsang, A. and Presti, S.L. (2004) March. 'Analysing the relationship between risk and trust.' In *International Conference on Trust Management*. Berlin Heidelberg: Springer, 135-145.

Jøsang, A., Ismail, R. and Boyd, C. (2007) 'A survey of trust and reputation systems for online service provision'. *Decision Support Systems 43*(2), 618-644.

Kahneman, D. (2003) 'A Perspective on judgment and choice: mapping bounded rationality'. *American Psychologist 58*(9), 697.

Kaiser, H.F. (1974) 'An index of factorial simplicity.' *Psychometrika 39*(1), 31-36.

Kanter, R.M. (1977) 'Some effects of proportions on group life'. In *The Gender Gap in Psychotherapy* ed. Kantor, R.M. Boston, MA: Springer, 53-78.

Kay, M.J. (2006) 'Strong brands and corporate brands'. *European Journal of Marketing 40*(7/8), 742-760.

Kee, H.W. and Knox, R.E. (1970) 'Conceptual and methodological considerations in the study of trust and suspicion'. *Journal of Conflict Resolution* 14(3), 357-366.

Keller, K.L. (1993) 'Conceptualizing, measuring, and managing customer-based brand equity.' *Journal of Marketing 57*(1), 1-22.

Kelman, H.C. (1961) 'Three processes of social influence.' *Public Opinion Quarterly 25*, 57-78.

Kenny, D.A. (1979) *Correlation and causality.* New York: Wiley.

Kesan, J.P. and Hayes, C.M. (2014) 'Creating a circle of trust to further digital privacy and cybersecurity goals'. *Mich. St. L. Rev.*, 1475.

Khan, K.M. and Malluhi, Q. (2010) 'Establishing trust in cloud computing.' *IT Professional*, *12*(5), pp.20-27.

Khodyakov, D. (2007) 'Trust as a process: A three-dimensional approach'. *Sociology 41*(1), 115-132.

Kim, P.H., Dirks, K.T., Cooper, C.D. and Ferrin, D.L. (2006) 'When more blame is better than less: The implications of internal vs. external attributions for the repair of trust after a competence-vs. integrity based trust violation'. *Organizational Behavior and Human Decision Processes 99*(1), 49-65.

Kim, D.J., Ferrin, D.L. and Rao, H.R. (2008) 'A Trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents.' *Decision Support Systems 44*(2), 544-564.

Kim, P.H., Dirks, K.T. and Cooper, C.D. (2009) 'The Repair of trust: A dynamic bilateral perspective and multilevel conceptualization.' *Academy of Management Review 34*(3), 401-422.

King-Casas, B., Tomlin, D., Anen, C., Camerer, C.F., Quartz, S.R. and Montague, P.R. (2005) 'Getting to know you: reputation and trust in a two-person economic exchange.' *Science*, *308*(5718), 78-83.

Kini, A. and Choobineh, J. (1998) January. 'Trust in electronic commerce: definition and theoretical considerations.' In *Proceedings of the thirty-first Hawaii International conference on System sciences.* IEEE. Vol. 4, 51-61.

Klein, T.J., Lambertz, C. and Stahl, K.O. (2016) 'Market transparency, adverse selection, and moral hazard'. *Journal of Political Economy*, *124*(6), 1677-1713.

Kline, R.B. (2005) *Principles and practice of structural equation modelling*. New York, NY: Guilford.

Knapp, K.J., Marshall, T.E., Kelly Rainer, R. and Nelson Ford, F. (2006) 'Information security: management's effect on culture and policy.' *Information Management & Computer Security 14*(1), 24-36.

Ko, M. and Dorantes, C. (2006) 'The impact of information security breaches on financial performance of the breached firms: an empirical investigation.' *Journal of Information Technology Management 17*(2), 13-22.

Koehler, J.J. and Gershoff, A.D. (2003) 'Betrayal aversion: When agents of protection become agents of harm.' *Organizational Behavior and Human Decision Processes 90*(2), 244-261.

Kolsaker, A. and Payne, C. (2002) 'Engendering trust in e-commerce: a study of gender-based concerns.' *Marketing Intelligence & Planning 20*(4), 206-214.

Kong, D.T., Dirks, K.T. and Ferrin, D.L. (2014) 'Interpersonal trust within negotiations: Meta-analytic evidence, critical contingencies, and directions for future research.' *Academy of Management Journal 57*(5), 1235-1255.

Korgaonkar, P.K. and Wolin, L.D. (1999) 'A multivariate analysis of web usage.' *Journal of Advertising Research 39*, 53-68.

Kreps, D.M. and Wilson, R. (1982) 'Reputation and imperfect information.' *Journal of Economic Theory 27*(2), 253-279.

Kreps, D.M. (1996) 'Corporate culture and economic theory.' In *Firms, Organizations and Contracts* ed. by Buckley,P and Mitchie,J. *, Oxford University Press, Oxford*, 221-275.

Krishnamurthy, S. (2001) 'A comprehensive analysis of permission marketing.' *Journal of Computer-Mediated Communication 6*(2), 623.

Kuhn, T.S. (1974) 'Second thoughts on paradigms.' In *The structure of scientific theories*, *2*, 459-482.

Kuhn, T.S. ([1962], 2012) *The structure of scientific revolutions*. University of Chicago press.

Lauer, T.W. and Deng, X. (2007) 'Building online trust through privacy practices.' *International Journal of Information Security 6*(5), 323-331.

Ledyard, O., 1995. Public goods: some experimental results. *Handbook of experimental economics*, *1*. Princeton University Press.

Lee, B.C., Ang, L. and Dubelaar, C. (20050 'Lemons on the Web: A signalling approach to the problem of trust in Internet commerce.' *Journal of Economic Psychology 26*(5), 607-623.

Lee, M.K. and Turban, E. (2001) 'A trust model for consumer internet shopping.' *International Journal of Electronic Commerce 6*(1), 75-91.

Lenard, P.T. (2008) 'Trust your compatriots, but count your change: The roles of trust, mistrust and distrust in democracy' *Political Studies 56*(2), 312-332.

Levitt, S.D. and Syverson, C. (2008) 'Market distortions when agents are better informed: The value of information in real estate transactions.' *The Review of Economics and Statistics 90*(4), 599-611.

Lewicki, R.J. and Bunker, B.B. (1996) 'Developing and maintaining trust in work relationships.' In *Trust in organizations: Frontiers of theory and research* eds. Kramer, R.M. and Tyler, T.R. Sage Publications, 139.

Lewis, J.D. and Weigert, A. (1985) 'Trust as a social reality.' *Social Forces 63*(4), 967-985.

Lewis, K. (2011) 'The co-evolution of social network ties and online privacy behavior.' In *Privacy online*. Springer, Berlin, Heidelberg, 91-109.

Lin, N. (1999) 'Building a network theory of social capital.' *Connections 22*(1), 28-51.

Lindell, M.K. and Perry, R.W. (2012) 'The Protective action decision model: theoretical modifications and additional evidence.' *Risk Analysis 32*(4), 616-632.

Liu, G., Wang, Y. and Orgun, M. (2009) August. 'Trust inference in complex trust-oriented social networks.' In *Computational Science and Engineering, 2009. CSE'09. International Conference on* (Vol. 4). IEEE, 996-1001.

Liu, R.Y., Parelius, J.M. and Singh, K (1999) 'Multivariate analysis by data depth: descriptive statistics, graphics and inference, (with discussion and a rejoinder by Liu and Singh).' *The Annals of Statistics 27*(3), 783-858.

Loader, I. and Walker, N. (2007) *Civilizing security*. Cambridge University Press.

Losee, R.M. (1997) 'A discipline independent definition of information.' *Journal of the American Society for information Science 48*(3), 254-269.

Luhmann, N. (2018) *Trust and power*. John Wiley & Sons.

Luhmann, Niklas (2000) 'Familiarity, Confidence, Trust: Problems and Alternatives', in Gambetta, Diego (ed.) Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford, chapter 6, 94-107.

Lukacs, Paul M., William L. Thompson, William L. Kendall, William R. Gould, Paul F. Doherty Jr, Kenneth P. Burnham, and David R. Anderson. 'Concerns regarding a call for pluralism of information theory and hypothesis testing.' *Journal of Applied Ecology* 44, no. 2 (2007), 456-460.

Lyons, B. and Mehta, J. (1997) 'Contracts, opportunism and trust: self-interest and social orientation.' *Cambridge Journal of Economics 21*(2), 239-257.

MacKenzie, S.B. and Podsakoff, P.M. (2012) 'Common method bias in marketing: causes, mechanisms, and procedural remedies.' *Journal of Retailing 88*(4), 542-555.

MacKinnon, D.P., Lockwood, C.M. and Williams, J. (2004) 'Confidence limits for the indirect effect: Distribution of the product and resampling methods.' *Multivariate Behavioral Research 39*(1), 99-128.

Madden, T.J., Ellen, P.S. and Ajzen, I. (1992) 'A comparison of the theory of planned behavior and the theory of reasoned action.' *Personality and social psychology Bulletin 18*(1), 3-9.

Maguire, S. and Phillips, N. (2008) ''Citibankers' at Citigroup: a study of the loss of institutional trust after a merger.' *Journal of Management Studies 45*(2), 372-401.

Mailath, G.J. (1998) 'Do people play Nash equilibrium? Lessons from evolutionary game theory.' *Journal of Economic Literature 36*(3), 1347-1374.

Malbon, J. (2013) 'Taking fake online consumer reviews seriously.' *Journal of Consumer Policy 36*(2), 139-157.

Malhotra, D. and Murnighan, J.K. (2002) 'The effects of contracts on interpersonal trust.' *Administrative Science Quarterly 47*(3), 534-559.

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004) 'Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model.' *Information Systems Research 15*(4), 336-355.

Mallach, E. (2000) *Decision Support and Data Warehouse Systems.* McGraw Hill.

Mallinckrodt, B., Abraham, W.T., Wei, M. and Russell, D.W. (2006) 'Advances in testing the statistical significance of mediation effects.' *Journal of Counseling Psychology 53*(3), 372.

Manktelow, K.I. and Over, D.E. (1991) 'Social roles and utilities in reasoning with deontic conditionals.' *Cognition 39*(2), 85-105.

Mármol, F.G. and Pérez, G.M. (2009) 'Security threats scenarios in trust and reputation models for distributed systems.' *Computers & Security 28*(7), 545-556.

Marsh, H.W., Balla, J.R. and Hau, K.T. (1996) 'An evaluation of incremental fit indices: A clarification of mathematical and empirical properties.' *Advanced Structural Equation Modeling: Issues and Techniques*, 315-353.

Marsh, S.P. (1994) *Formalising trust as a computational concept.* PhD Thesis, Stirling University.

Martin, G., Kinross, J. and Hankin, C. (2017) Effective cybersecurity is fundamental to patient safety. British Medical Journal , 237. [online] https://spiral.imperial.ac.uk/bitstream/10044/1/49096/2/cyber.pdf [16th July 2019].

Maslow, A.H. (1943) 'A theory of human motivation.' *Psychological review 50*(4), 370.

Mayer, R.C., Davis, J.H. and Schoorman, F.D. (1995) 'An integrative model of organizational trust.' *Academy of Management Review 20*(3), 709-734.

Mayer, R.C. and Davis, J.H. (1999) 'The Effect of the performance appraisal system on trust for management: A field quasi-experiment.' *Journal of Applied Psychology 84*(1), 123.

McAllister, D.J. (1995) 'Affect-and cognition-based trust as foundations for interpersonal cooperation in organizations.' *Academy of Management Journal 38*(1), 24-59.

McCarthy, J. and Hayes, P.J. (1981) 'Some philosophical problems from the standpoint of artificial intelligence'. In *Readings in artificial intelligence* Morgan Kauffmann, 431-450.

McConnell-Henry, T., Chapman, Y. and Francis, K. (2009) 'Unpacking Heideggerian phenomenology.' *Southern Online Journal of Nursing Research 9*(1), 1-11.

McGoey, L. (2012) 'The logic of strategic ignorance.' *The British Journal of Sociology 63*(3), 533-576.

McKnight, D.H, N.L.C. (2001) 'What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology.' *International Journal of Electronic Commerce 6*(2), 35-59.

McKnight, D.H. and Chervany, N.L. (2000) 'What is trust? A conceptual analysis and an interdisciplinary model.' *AMCIS 2000 Proceedings*, 382.

McKnight, D.H. and Chervany, N.L. (2001) Trust and distrust definitions: One bite at a time. In *Trust in Cyber-societies* eds. R. Falcone, M. Singh and Y. H. Tan. Berlin Heidelberg: Springer, 27-54

McKnight, D.H., Choudhury, V. and Kacmar, C. (2002) 'The impact of initial consumer trust on intentions to transact with a web site: a trust building model.' *The Journal of Strategic Information Systems 11*(3-4), 297-323.

McKnight, D.H., Cummings, L.L. and Chervany, N.L. (1998) 'Initial trust formation in new organizational relationships.' *Academy of Management Review 23*(3), 473-490.

McMahan, H.B., Holt, G., Sculley, D., Young, M., Ebner, D., Grady, J., Nie, L., Phillips, T., Davydov, E., Golovin, D. and Chikkerur, S. (2013) August. 'Ad click prediction: a view from the trenches.' In *Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining.* ACM, 1222-1230.

Mead, G.H. (1934) *Mind, self and society* (Vol. 111). University of Chicago Press: Chicago.

Mellewigt, T., Madhok, A. and Weibel, A. (2007) 'Trust and formal contracts in interorganizational relationships—substitutes and complements.' *Managerial and Decision Economics 28*(8), 833-847.

Merendino, A., Dibb, S., Meadows, M., Quinn, L., Wilson, D., Simkin, L. and Canhoto, A. (2018) 'Big data, big decisions: The impact of big data on board level decision-making.' *Journal of Business Research 93*, 67-78.

Mertens, D.M. (2007) 'Transformative paradigm: Mixed methods and social justice.' *Journal of Mixed Methods Research 1*(3), 212-225.

Mietzner, S. and Li-Wen, L. (2005) 'Would you do it again? Relationship skills gained in a long-distance relationship.' *College Student Journal 39*(1), 192-198.

Mikulincer, M., Shaver, P.R. and Pereg, D. (2003) 'Attachment theory and affect regulation: The dynamics, development, and cognitive consequences of attachment-related strategies.' *Motivation and Emotion 27*(2), 77-102.

Miller, G.A. (1956) 'The magical number seven, plus or minus two: some limits on our capacity for processing information.' *Psychological Review 63*(2), 81.

Milne, G.R., Rohm, A.J. and Bahl, S. (2004) 'Consumers' protection of online privacy and identity.' *Journal of Consumer Affairs 38*(2), 217-232.

Mingers, J. (2003) ‘A classification of the philosophical assumptions of management science methods.’ *Journal of the Operational Research Society 54*(6), 559-570.

Mitchell, L.E. (1990) ‘The Death of Fiduciary Duty in Close Corporations.’ *University of Pennsylvania Law Review 138*(6), 1675-1731.

Miyazaki, A.D. and Fernandez, A. (2001) ‘Consumer perceptions of privacy and security risks for online shopping.’ *Journal of Consumer Affairs 35*(1), 27-44.

Molm, L.D., Takahashi, N. and Peterson, G. (2000) ‘Risk and trust in social exchange: An experimental test of a classical proposition.’ *American Journal of Sociology 105*(5), 1396-1427.

Moore, G.E. (2014) *Some main problems of philosophy*. Routledge.

Moorman, C., Zaltman, G. and Deshpande, R. (1992) ‘Relationships between providers and users of market research: The dynamics of trust within and between organizations.’ *Journal of Marketing Research 29*(3), 314.

Moorman, R.H., Blakely, G.L. and Niehoff, B.P. (1998) ‘Does perceived organizational support mediate the relationship between procedural justice and organizational citizenship behavior?’ *Academy of Management Journal 41*(3), 351-357.

Morgan, R.M. and Hunt, S.D. (1994) ‘The commitment-trust theory of relationship marketing.’ *The Journal of Marketing*, 20-38.

Mutz, D.C. (2005) ‘Social trust and e-commerce: Experimental evidence for the effects of social trust on individuals’ economic behavior.’ *Public Opinion Quarterly 69*(3), 393-416.

Myers, I.B., McCaulley, M.H., Quenk, N.L. and Hammer, A.L. (2003) *MBTI Manual: A Guide to the Development and Use of the Myers-Briggs Type Indicator, 3rd*. Palo Alto, CA: Consulting Psychologists Press.

NAO (2019) Progress of the UK Cyber Security Programme 2016-21. National Audit Office UK. [online] https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-Cyber-Security-Programme.pdf [15th June 2019].

nCipher.com (2019) nCipher Security Survey on trust in online scenarios. https://www.helpnetsecurity.com/2019/04/26/consumers-trust-banks-most-with-their-personal-data/ [15th June 2019].

Nekmat, E. and Gower, K.K. (2012) 'Effects of disclosure and message valence in online word-of-mouth (eWOM) communication: implications for integrated marketing communication.' *International Journal of Integrated Marketing Communications 4*(1), 85-98.

Netemeyer, R.G., Krishnan, B., Pullig, C., Wang, G., Yagci, M., Dean, D., Ricks, J. and Wirth, F. (2004) 'Developing and validating measures of facets of customer-based brand equity.' *Journal of Business Research 57*(2), 209-224.

Newell, A. and Simon, H.A. (1972) *Human problem solving* (Vol. 104, No. 9). Englewood Cliffs, NJ: Prentice-Hall.

Newman, I., Benz, C.R. and Ridenour, C.S. (1998) *Qualitative-quantitative research methodology: Exploring the interactive continuum*. SIU Press.

Niehoff, B.P. and Moorman, R.H. (1993) 'Justice as a mediator of the relationship between methods of monitoring and organizational citizenship behavior.' *Academy of Management Journal 36*(3), 527-556.

Nissenbaum, H. (2004) 'Privacy as contextual integrity.' *Wash. L. Rev. 79*, 119.

Noe, T.H. and Rebello, M.J. (1996) 'Asymmetric information, managerial opportunism, financing, and payout policies.' *The Journal of Finance 51*(2), 637-660.

Nunnally, J.C. and Bernstein, I.H. (1994) *Psychological theory*. *New York, NY: MacGraw-Hill*, 131-147.

Nunnally, J.C., Bernstein, I.H. and Berge, J.M.T. (1967) *Psychometric theory* (Vol. 226). New York: McGraw-Hill.

Nurse, J.R., Creese, S., Goldsmith, M. and Lamberts, K. (2011) September. 'Trustworthy and effective communication of cybersecurity risks: A review.' In *Socio-Technical Aspects in Security and Trust (STAST), 2011 1st Workshop*. IEEE, 60-68.

Nyaga, G.N., Lynch, D.F., Marshall, D. and Ambrose, E. (2013) 'Power asymmetry, adaptation and collaboration in dyadic relationships involving a powerful partner.' *Journal of Supply Chain Management 49*(3), 42-65.

OED (2019) Dictionary definition by Oxford English Dictionary [online]. https://www.lexico.com/en/definition/epistemology [15th June 2019].

O'Neill, O. (2002) *A question of trust: The BBC Reith Lectures 2002*. Cambridge University Press.

ONS (2017) Office for National Statistics, UK. Mid-year estimates, 2017 [online]. https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/bulletins/annualmidyearpopulationestimates/mid2017 [15th June 2019].

Oppenheim, A.N. (2000) *Questionnaire design, interviewing and attitude measurement*. Bloomsbury Publishing.

Origgi, G. (2004) 'Is trust an epistemological notion?' *Episteme 1*(01), 61-72.

Osborne, J.W., Costello, A.B. and Kellow, J.T. (2008) 'Best practices in exploratory factor analysis.' *Best practices in quantitative methods*, 86-99.

Ostrom, E. (1998) 'A Behavioral approach to the rational choice theory of collective action: Presidential address, American Political Science Association, 1997.' *American Political Science Review 92*(1), 1-22.

Ostrom, E. (2014) 'Collective action and the evolution of social norms.' *Journal of Natural Resources Policy Research 6*(4), 235-252.

Osoba, O.A. and Welser IV, W. (2017) '*An intelligence in our image: The risks of bias and errors in Artificial Intelligence'*. Rand Corporation.

Panchanathan, K. and Boyd, R. (2003) 'A tale of two defectors: the importance of standing for evolution of indirect reciprocity.' *Journal of Theoretical Biology 224*(1), 115-126.

Pavlou, P.A. and Dimoka, A. (2006) 'The nature and role of feedback text comments in online marketplaces: Implications for trust building, price premiums, and seller differentiation.' *Information Systems Research 17*(4), 392-414.

Pavlou, P.A. and Fygenson, M. (2006) 'Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior.' *MIS Quarterly*, 115-143.

Pavlou, P.A. and Gefen, D. (2004) 'Building effective online marketplaces with institution-based trust.' *Information Systems Research*, *15*(1), 37-59.

Pavlou, P.A. (2003) 'Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model.' *International Journal of Electronic Commerce 7*(3), 101-134.

Pendse, S.G. (2012) 'Ethical hazards: A motive, means, and opportunity approach to curbing corporate unethical behavior.' *Journal of Business Ethics 107*(3), 265-279.

Phillips, J.T. (2002) 'Privacy vs. cybersecurity.' *Information Management 36*(3), 46.

Pinto, M.B., Pinto, J.K. and Prescott, J.E. (1993) 'Antecedents and consequences of project team cross-functional cooperation.' *Management Science 39*(10), 1281-1297.

Pomazal, R.J. and Jaccard, J.J. (1976) 'An informational approach to altruistic behavior.' *Journal of Personality and Social Psychology 33*(3) p.317.

Popper, K. (2005) *The logic of scientific discovery*. Routledge.

Power, D. and Singh, P. (2007) 'The e-integration dilemma: The linkages between Internet technology application, trading partner relationships and structural change.' *Journal of Operations Management 25*(6), 1292-1310.

Pratt, J.W. ed. (1991) *Principals and agents: The structure of business*. Boston, MA: Harvard Business School Press.

Preacher, K.J. and Hayes, A.F. (2004) 'SPSS and SAS procedures for estimating indirect effects in simple mediation models.' *Behavior Research Methods, Instruments, & Computers 36*(4), 717-731.

Preacher, K.J. and Hayes, A.F. (2008) 'Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models.' *Behavior Research Methods 40*(3), 879-891.

Prescott, E.C. and Townsend, R.M. (1984) 'Pareto optima and competitive equilibria with adverse selection and moral hazard.' *Econometrica: Journal of the Econometric Society* 52(1), 21-45.

Probst, T.M. (2003) 'Development and validation of the job security index and the job security satisfaction scale: A classical test theory and IRT approach.' *Journal of Occupational and Organizational Psychology 76*(4), 451-467.

Putnam, R.D. (1995) 'Bowling alone: America's declining social capital.' *Journal of Democracy 6*(1), 65-78.

Rabin, M. (1993) 'Incorporating fairness into game theory and economics.' *The American Economic Review* 83(5), 1281-1302.

Ramakrishnan, R.T. and Thakor, A.V. (1984) 'Information reliability and a theory of financial intermediation.' *The Review of Economic Studies 51*(3), 415-432.

Ratnasingam, P., Pavlou, P.A. and Tan, Y.H. (2002) June. 'The importance of technology trust for B2B electronic commerce.' In *15th Bled Electronic Commerce Conference eReality: Constructing the eEconomy, Bled, Slovenia*. BLED 2002 Proceedings, 31-43.

Raykov, T. and Marcoulides, G.A. (1999) 'On desirability of parsimony in structural equation model selection.' *Structural Equation Modeling: A Multidisciplinary Journal 6*(3), 292-300.

Raykov, T. (1997) 'Estimation of composite reliability for congeneric measures.' *Applied Psychological Measurement 21*(2), 173-184.

Remenyi, D., Williams, B., Money, A. and Swartz, E. (1998) *Doing research in business and management: an introduction to process and method*. Sage.

Rempel, J.K., Holmes, J.G. and Zanna, M.P. (1985) 'Trust in close relationships.' *Journal of Personality and Social Psychology 49*(1), 95.

Restubog, S.L.D., Hornsey, M.J., Bordia, P. and Esposo, S.R. (2008) 'Effects of psychological contract breach on organizational citizenship behaviour: Insights from the group value model.' *Journal of Management Studies 45*(8), 1377-1400.

Ricci, F., Rokach, L. and Shapira, B. (2015) 'Recommender systems: introduction and challenges.' In *Recommender Systems Handbook*. Boston, MA: Springer, 1-34.

Richardson, W.J. (2013) *Heidegger: Through phenomenology to thought*. Springer.

Riegelsberger, J. and Sasse, M.A. (2001) 'Trustbuilders and trustbusters'. In Schmid, B., Stanoevska-Slabeva, K. and Tschammer, V. eds., *Towards the E-Society: E-commerce, E-business, and E-government* (Vol. 74). Springer Science & Business Media, 17-30.

Riva, G., Teruzzi, T. and Anolli, L. (2003) 'The use of the internet in psychological research: comparison of online and offline questionnaires.' *CyberPsychology & Behavior 6*(1), 73-80.

Robert, L.P., Denis, A.R. and Hung, Y.T.C. (2009) 'Individual swift trust and knowledge-based trust in face-to-face and virtual team members.' *Journal of Management Information Systems 26*(2), 241-279.

Robinson, S.L. and Rousseau, D.M. (1994) 'Violating the psychological contract: Not the exception but the norm.' *Journal of Organizational Behavior 15*(3), 245-259.

Robinson, S. L., Dirks, K. T., & Ozcelik, H. (2004). Untangling the Knot of Trust and Betrayal. In R. M. Kramer & K. S. Cook (Eds.), *The Russell Sage Foundation series on trust. Trust and distrust in organizations: Dilemmas and approaches*. New York, NY, US: Russell Sage Foundation, 327-341.

Rokeach, M. (1968) 'The role of values in public opinion research. *Public Opinion Quarterly 32*(4), 547-559.

Rosenberg, S. and Park Kim, M. (1975) 'The method of sorting as a data-gathering procedure in multivariate research.' *Multivariate Behavioral Research 10*(4), 489-502.

Rossiter, J.R. (2002) 'The C-OAR-SE procedure for scale development in marketing.' *International Journal of Research in Marketing 19*(4), 305-335.

Rothrock, R.A., Kaplan, J. and Van Der Oord, F. (2018) 'The board's role in managing cybersecurity risks.' *MIT Sloan Management Review 59*(2), 12-15.

Rotter, J.B. (1967) 'A new scale for the measurement of interpersonal trust.' *Journal of Personality 35*(4), 651-665.

Rotter, J.B. (1980) 'Interpersonal trust, trustworthiness, and gullibility.' *American Psychologist 35*(1), 1.

Rousseau, D.M. and McLean Parks, J. (1993) 'The contracts of individuals and organizations.' *Research in Organizational Behavior 15*, 1-10.

Rousseau, D.M., Sitkin, S.B., Burt, R.S. and Camerer, C. (1998) 'Not so different after all: A cross-discipline view of trust.' *Academy of Management Review 23*(3), 393-404.

Rousseau, J.J. and May, G. ([1762], 2002) *The social contract: And, the first and second discourses*. Yale University Press.

Rowley, J. (2014) 'Designing and using research questionnaires.' *Management Research Review 37*(3), 308-330.

Roy, S.K., Devlin, J., Sekhon, H. and Bian, X. (2019) 'Decision Delegation and Trust: Insights from Financial Services.' In Academy of Marketing Science World Marketing Congress 2019: Enlightened Marketing in Challenging Times, Edinburgh, UK. (In Press)

Rucker, D.D., Preacher, K.J., Tormala, Z.L. and Petty, R.E. (2011) 'Mediation analysis in social psychology: Current practices and new recommendations.' *Social and Personality Psychology Compass 5*(6), 359-371.

Rudner, R. (1953) 'The scientist qua scientist makes value judgments.' *Philosophy of Science 20*(1), 1-6.

Russell, S., Hauert, S., Altman, R. and Veloso, M. (2015) 'Ethics of artificial intelligence.' *Nature 521*(7553), 415-416.

Salisbury, W.D., Pearson, R.A., Pearson, A.W. and Miller, D.W. (2001) 'Perceived security and World Wide Web purchase intention.' *Industrial Management & Data Systems 101*(4), 165-177.

Sample, C. and Karamanian, A. (2015) July. 'Culture and cyber behaviours: DNS defending.' In *Proceedings of the 14th European Conference on Cyber Warfare and Security,* 233-242.

Sanquist, T.F., Mahy, H. and Morris, F. (2008) 'An exploratory risk perception study of attitudes toward homeland security systems.' *Risk Analysis 28*(4), 1125-1133.

Sarkar, M., Butler, B. and Steinfield, C. (1998) 'Cybermediaries in electronic marketspace: toward theory building.' *Journal of Business Research 41*(3), 215-221.

Savolainen, T. and Fresno, P.L. (2013) 'Trust as intangible asset-enabling intellectual capital development by leadership for vitality and innovativeness.' *Electronic Journal of Knowledge Management 11*(3), 244.

Schermelleh-Engel, K., Moosbrugger, H. and Müller, H. (2003) 'Evaluating the fit of structural equation models: Tests of significance and descriptive goodness-of-fit measures.' *Methods of Psychological Research Online 8*(2), 23-74.

Schilke, O. and Cook, K.S. (2015) 'Sources of alliance partner trustworthiness: Integrating calculative and relational perspectives.' *Strategic Management Journal 36*(2), 276-297.

Schoeman, F.D. (1984) *Philosophical dimensions of privacy: An anthology*. Cambridge University Press.

Schoorman, F.D., Mayer, R.C. and Davis, J.H. (2007) 'An integrative model of organizational trust: Past, present, and future.' *Academy of Management Review 32*(2), 344-354.

Schoorman, F.D., Mayer, R.C. and Davis, J.H. (2016) 'Empowerment in veterinary clinics: The role of trust in delegation.' *Journal of Trust Research 6*(1), 76-90.

Schwandt, T.A. (1994) 'Constructivist, interpretivist approaches to human inquiry.' *Handbook of qualitative research*, *1*, 118-137.

Searle, J.R. and Willis, S. (1995) *The construction of social reality*. Simon and Schuster.

Searle, J.R. (1980) 'Minds, brains, and programs.' *Behavioral and Brain Sciences 3*(3), 417-424.

Searle, J.R. (1983) *Intentionality: An essay in the philosophy of mind*. Cambridge University Press.

Sekhon, H., Ennew, C., Kharouf, H. and Devlin, J. (2014) 'Trustworthiness and trust: Influences and implications.' *Journal of Marketing Management 30*(3-4), 409-430.

Seligman, A.B. (1997) *The problem of trust*. Princeton University Press.

Sen, R. and Borle, S. (2015) 'Estimating the contextual risk of data breach: An empirical approach.' *Journal of Management Information Systems 32*(2), 314-341.

Shannon, C.E. ([1948], 2001) 'A mathematical theory of communication.' *ACM SIGMOBILE mobile computing and communications review 5*(1), 3-55.

Shao, B., Wang, D., Li, T. and Ogihara, M. (2009) 'Music recommendation based on acoustic features and user access patterns.' *IEEE Transactions on Audio, Speech, and Language Processing 17*(8), 1602-1611.

Shapiro, D.L., Sheppard, B.H. and Cheraskin, L. (1992) 'Business on a handshake.' *Negotiation Journal 8*(4), 365-377.

Shapiro, S.P. (1987) 'The social control of impersonal trust.' *American Journal of Sociology*, 623-658.

Sheather, S.J. (2009) Variable Selection. In Casella, G., Fienberg, S.I.O. and Olkin, I., eds. *A Modern Approach to Regression with R*. Springer, New York, NY, 227-261.

Sheppard, B.H. and Sherman, D.M. (1998) ‘The grammars of trust: A model and general implications.’ *Academy of Management Review 23*(3), 422-437.

Shrout, P.E. and Bolger, N. (2002) ‘Mediation in experimental and non-experimental studies: new procedures and recommendations.’ *Psychological Methods 7*(4), 422.

Siegrist, M., Cvetkovich, G. and Roth, C. (2000) 'Salient value similarity, social trust, and risk/benefit perception.’ *Risk Analysis 20*(3), 353-362.

Silvia, E.S.M. and MacCallum, R.C. (1988) ‘Some factors affecting the success of specification searches in covariance structure modeling.’ *Multivariate Behavioral Research 23*(3), 297-326.

Simon, H.A. (1955) ‘A behavioral model of rational choice.’ *The Quarterly Journal of Economics 69*(1), 99-118.

Simon, H.A. (1972) ‘Theories of bounded rationality.’ *Decision and Organization 1*(1), 161-176.

Sirdeshmukh, D., Singh, J. and Sabol, B. (2002) ‘Consumer trust, value, and loyalty in relational exchanges.’ *Journal of Marketing 66*(1), 15-37.

Smith, J.A. (1996) ‘Beyond the divide between cognition and discourse: Using interpretative phenomenological analysis in health psychology.’ *Psychology and Health 11*(2), 261-271.

Smith, M.L. (2006) ‘Overcoming theory-practice inconsistencies: Critical realism and information systems research.’ *Information and Organization 16*(3), 191-211.

Sniehotta, F.F. (2009) ‘Towards a theory of intentional behaviour change: Plans, planning, and self-regulation.’ *British Journal of Health Psychology 14*(2), 261-273.

Sommestad, T. and Hallberg, J. (2013) July. 'A review of the theory of planned behaviour in the context of information security policy compliance.' In *IFIP International Information Security Conference* Berlin, Heidelberg: Springer, 257-271.

Spencer, D. and Warfel, T. (2004) *Card sorting: a definitive guide.* Boxes and arrows.

Sperber, D., Clément, F., Heintz, C., Mascaro, O., Mercier, H., Origgi, G. and Wilson, D. (2010) 'Epistemic vigilance.' *Mind & Language 25*(4), 359-393.

Srinivasan, S.S. and Till, B.D. (2002) 'Evaluation of search, experience and credence attributes: role of brand name and product trial.' *Journal of Product & Brand Management 11*(7), 417-431.

Statista.com (2018) https://www.statista.com/statistics/326169/united-kingdom-uk-online-banking-losses/ Accessed 15th June 2019.

Statista.com (2019) Value of annual online banking fraud losses in United Kingdom (UK) from 2010 to 2017. [online] https://www.statista.com/topics/2333/e-commerce-in-the-united-kingdom/ [15th June 2019].

Steenkamp, J.B.E., De Jong, M.G. and Baumgartner, H. (2010) 'Socially desirable response tendencies in survey research.' *Journal of Marketing Research 47*(2), 199-214.

Steinhardt, J., Koh, P.W.W. and Liang, P.S. (2017) 'Certified defenses for data poisoning attacks.' In *Advances in neural information processing systems,* 3517-3529.

Stine, R. (1989) 'An introduction to bootstrap methods: Examples and ideas.' *Sociological Methods & Research 18*(2-3), 243-291.

Suh, B. and Han, I. (2003) 'The impact of customer trust and perception of security control on the acceptance of electronic commerce.' *International Journal of Electronic Commerce 7*(3), 135-161.

Sun, Y., Han, Z. and Liu, K.R. (2008) 'Defense of trust management vulnerabilities in distributed networks.' *IEEE Communications Magazine 46*(2), 112-119.

Sunstein, C.R. (1996) 'Social norms and social roles.' *Columbia law review 96*(4), 903-968.

Sweeney, L. (2002) 'k-anonymity: A model for protecting privacy.' *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10*(05), 557-570.

Swift.com (2019) SWIFT financial messaging. [online] https://www.swift.com/news-events/press-releases/swift-report-gives-new-insights-into-cyber-threats [15th June 2019].

Sztompka, P. (1999) *Trust: A sociological theory*. Cambridge University Press.

Sztompka, P. (2000) 'Trust, distrust and the paradox of democracy.' *Polish Pol. Sci. YB*, *29*, 5.

Tajfel, H. and Turner, J.C. (1979) 'An integrative theory of intergroup conflict.' *The Social Psychology of Intergroup Relations 33*(47), 74.

Tan, Y.H. and Thoen, W. (2000) 'An outline of a trust model for electronic commerce.' *Applied Artificial Intelligence 14*(8), 849-862.

Tavakol, M. and Dennick, R. (2011) 'Making sense of Cronbach's alpha.' *International Journal of Medical Education*, *2*, 53.

Tesser, A. and Leone, C. (1977) 'Cognitive schemas and thought as determinants of attitude change.' *Journal of Experimental Social Psychology 13*(4), 340-356.

Thurstone, L.L. (1931) 'Multiple factor analysis.' *Psychological Review 38*(5), 406.

Tilley, J.J. (2004) 'Justifying reasons, motivating reasons, and agent relativism in ethics.' *Philosophical Studies 118*(3), 373-399.

Tinsley, H.E. and Tinsley, D.J. (1987) 'Uses of factor analysis in counseling psychology research.' *Journal of Counseling Psychology 34*(4), 414.

Tipton, H.F. and Henry, K. eds. (2006) *Official (ISC) 2 guide to the CISSP CBK*. Auerbach Publications.

Tomkins, C. (2001) 'Interdependencies, trust and information in relationships, alliances and networks.' *Accounting, Organizations and Society 26*(2), 161-191.

Tooze, A. (2018) *Crashed: How a decade of financial crises changed the world*. Penguin.

Tranfield, D. and Starkey, K. (1998) 'The nature, social organization and promotion of management research: Towards policy.' *British Journal of Management 9*(4), 341-353.

Tsiakis, T. and Stephanides, G. (2005) 'The economic approach of information security.' *Computers & Security 24*(2), 105-108.

Tucker, L.R. and Lewis, C. (1973) 'A reliability coefficient for maximum likelihood factor analysis.' *Psychometrika 38*(1), 1-10.

Van de Walle, S., Van Roosbroek, S. and Bouckaert, G. (2008) 'Trust in the public sector: is there any evidence for a long-term decline?' *International Review of Administrative Sciences 74*(1), 47-64.

Van der Heijden, H., Verhagen, T. and Creemers, M. (2003) 'Understanding online purchase intentions: contributions from technology and trust perspectives.' *European Journal of Information Systems 12*(1), 41-48.

Vanneste, B.S., Puranam, P. and Kretschmer, T. (2014) 'Trust over time in exchange relationships: Meta-analysis and theory.' *Strategic Management Journal 35*(12), 1891-1902.

Venkatesh, V. and Davis, F.D. (2000) 'A theoretical extension of the technology acceptance model: Four longitudinal field studies.' *Management Science 46*(2), 186-204.

Vishik, C. and Balduccini, M. (2015) 'Making sense of future cybersecurity technologies: using ontologies for multidisciplinary domain analysis.' In *ISSE 2015* Vieweg, Wiesbaden: Springer, 135-145.

Vogt, W.P. and Johnson, B. (2011) *Dictionary of statistics & methodology: A nontechnical guide for the social sciences*. Sage.

Von Solms, R. and Van Niekerk, J. (2013) 'From information security to cyber security.' *Computers & Security*, *38*, 97-102.

Wanderer, J. and Townsend, L. (2013) Is it rational to trust?' *Philosophy Compass 8*(1), 1-14.

Wang, S., Beatty, S.E. and Foxx, W. (2004) 'Signaling the trustworthiness of small online retailers.' *Journal of Interactive Marketing 18*(1), 53-69.

Warfield, D., 2010. 'IS/IT Research: A Research Methodologies Review.' *Journal of Theoretical & Applied Information Technology 13*, 28-35.

Wasserstein, R.L. and Lazar, N.A. (2016) 'The ASA's statement on p-values: context, process, and purpose.' *The American Statistician 70*(2), 129-133.

Waterman, R.W. and Meier, K.J. (1998) 'Principal-agent models: an expansion?' *Journal of Public Administration Research and Theory 8*(2), 173-202.

Weiss, G.M. and Provost, F. (2003) 'Learning when training data are costly: The effect of class distribution on tree induction.' *Journal of Artificial Intelligence Research 19*, 315-354.

Westfall, P.H. (2014) 'Kurtosis as peakedness, 1905–2014. RIP.' *The American Statistician 68*(3), 191-195.

Whaley, A.L. and Longoria, R.A. (2009) 'Preparing card sort data for multidimensional scaling analysis in social psychological research: a methodological approach.' *The Journal of Social Psychology 149*(1), 105-115.

Whetten, D.A. (1989) 'What constitutes a theoretical contribution?' *Academy of Management Review 14*(4), 490-495.

Whitener, E.M., Brodt, S.E., Korsgaard, M.A. and Werner, J.M. (1998) 'Managers as initiators of trust: An exchange relationship framework for understanding managerial trustworthy behavior.' *Academy of Management Review 23*(3), 513-530.

Wicks, A.C., Berman, S.L. and Jones, T.M. (1999) 'The structure of optimal trust: Moral and strategic implications.' *Academy of Management Review 24*(1), 99-116.

Wikihow.com (2019) Fake online Reviews [online] https://www.wikihow.com/Spot-a-Fake-Review-on-Amazon. [15th June 2019].

Wildschut, T., Sedikides, C., Arndt, J. and Routledge, C. (2006) 'Nostalgia: content, triggers, functions.' *Journal of Personality and Social Psychology 91*(5), 975.

Williamson, O.E. (1993) 'Calculativeness, trust, and economic organization.' *The Journal of Law & Economics 36*(1), 453-486.

Witten, I.H., Frank, E., Hall, M.A. and Pal, C.J. (2016) *Data Mining: Practical machine learning tools and techniques*. Morgan Kaufmann.

Wright, A. and Ehnert, I. (2010) 'Making sense of trust across cultural contexts.' *Organizational trust: A cultural perspective*, 107-126.

Wright, S. (2010) 'Trust and trustworthiness.' *Philosophia 38*(3), 615-627.

Xiang, Z. and Gretzel, U. (2010) 'Role of social media in online travel information search.' *Tourism Management 31*(2), 179-188.

Xiong, L. and Liu, L. (2003) June. 'A reputation-based trust model for peer-to-peer e-commerce communities.' In *EEE International Conference on E-Commerce, 2003. CEC 2003.* IEEE, 275-284.

Xiong, L. and Liu, L. (2004) 'Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities.' *IEEE transactions on Knowledge and Data Engineering 16*(7), 843-857.

Yamagishi, T. and Yamagishi, M. (1994) 'Trust and commitment in the United States and Japan'. *Motivation and Emotion 18*(2), 129-166.

Yamagishi, T., Kanazawa, S., Mashima, R. and Terai, S. (2005) 'Separating trust from cooperation in a dynamic relationship prisoner's dilemma with variable dependence.' *Rationality and Society 17*(3), 275-308.

Yang, J., Hu, X. and Zhang, H. (2007) 'Effects of a reputation feedback system on an online consumer-to-consumer auction market.' *Decision Support Systems 44*(1), 93-105.

Zak, P.J. (2008) 'The neurobiology of trust.' *Scientific American 298*(6), 88-95.

Zand, D.E. (1972) 'Trust and managerial problem solving.' *Administrative Science Quarterly*, 229-239.

Zhao, S., Grasmuck, S. and Martin, J. (2008) 'Identity construction on Facebook: Digital empowerment in anchored relationships.' *Computers in Human Behavior 24*(5), 1816-1836.

Zhao, X., Lynch Jr, J.G. and Chen, Q. (2010) 'Reconsidering Baron and Kenny: Myths and truths about mediation analysis.' *Journal of Consumer Research 37*(2), 197-206.

Zhou, X., Xu, Y., Li, Y., Josang, A. and Cox, C. (2012) 'The state-of-the-art in personalized recommender systems for social networking.' *Artificial Intelligence Review 37*(2), 119-132.

Zhu, Y.Q. and Chang, J.H. (2016) 'The key role of relevance in personalized advertisement: Examining its impact on perceptions of privacy invasion, self-awareness, and continuous use intentions.' *Computers in Human Behavior 65*, 442-447.

Zucker, L.G. (1986) 'Production of trust: Institutional sources of economic structure, 1840-1920.' *Research in Organizational Behavior 8*, 53-111.

Appendices

The following items have been included as appendices to this work, and are referenced within the main text of the thesis.

- Appendix A1. Full listing of raw items, item stems and rationale for the item generation.
- Appendix A2. Sample Banking Scenario Questionnaire.
- Appendix A3. Sample output from AMOS modelling for CFA and SEM.

Appendix A1: Item Generation

Items were generated based on prior literature with new items included where it was judged that existing scales or items did not effectively describe the research situation. The initial conceptual model contained eight constructs, two of which (privacy and vulnerability protection) were dropped as part of the EFA and CFA analysis as they displayed poor levels of discriminant and construct validity. The question items that were included in the validated research model are highlighted.

Security							
Item	**First Order**	**Second Order**	**Item Stem**	**Item Scale**	**Rationale**	**Source**	**Inclusion Rationale**
S1	**Role**	**Confidentiality**	The trustee organisation should protect the Relationship from external threats.	5 Point Likert scale Very Important to Not important	The Physical security measures taken by organisations represent the manifest exogenous 'behaviour' of security, as opposed to the underlying theme of psychological safety and freedom from harm. A 'New' scale incorporating the variables relevant to sense of security is required.	Agarawal, 2011	Role of Security
S2	**Psychological Safety**	**Security Controls**	I feel safe from cyber threats and their effects	5 point likert Scale Not Safe to Very Safe		Maslow; OSSTMM	Relates to self not information
S3		**Separation**	I feel confident that my assets, information are	5 point likert Scale Not Safe to Very Safe		OSSTMM	InfoSec

			safe from external threats				
S4			I feel that there is a balance between safety and the controls in place to combat threats	Yes/ No	New Scale	OSSTMM	Balance between power and safety
S5		**Confidence**	I feel confident that I am personally / my assets/ vulnerabilities are safe from threats	5 point likert Scale Not Safe to Very Safe	New Scale	OSSTMM	Same as S3
S6		**Identity**	I feel that my identity is maintained securely from external cyber threats by the trustee	5 point likert Scale Not Safe to Very Safe	New Scale	*New	Vulnerability, not Security ?
S7	**Task**	**Importance**	I feel sure about undertaking this task online. [Reworded to I feel sure that the use of online systems is appropriate to this task.]	JSI	Adapted JSI Scale: JSI 1. Sure,2. Unpredictable,4. Secure,5. Stable,6. Questionable,8. Well Established,9. Almost Guaranteed,10. Uncertain,13. Unclear,15. Certain,16. Temporary, 18. Insecure	Adapted from Probst(2001) Effects of Job insecurity on safety outcomes	Adapt the Job Security Index to attain a measurement of confidence in the security of the participant. Too general, reworded
S8		**Threat to task / loss**	There is a risk of loss in completing this task online.	JSI		Adapted from Probst(2001) Effects of Job	Vulnerability, not Security ?

						insecurity on safety outcomes	
S9		**Powerlessness**	I am unable to influence the presence of threats inherent in the task.	JSI		Adapted from Probst(2001) Effects of Job insecurity on safety outcomes	Authority of protector
S10		**Justice**	I have the possibility of redress in the event of task failure due to cyber threat.	JSI		Adapted from Probst(2001) Effects of Job insecurity on safety outcomes	Importance
S11	**Policy**	**CyberSecurity**	The providers information policy is well known	True/False/Unknown	CISSP InfoSec policy (Ref)	Adapted from Knapp et al, 2006 (200 cites)	Not Relevant
S12			I feel that employees caught violating important security policies are appropriately corrected	True/False/Unknown		Adapted from Knapp et al, 2006 (200 cites)	Not Relevant
S13			I feel that security policies are properly monitored for violations	True/False/Unknown		Adapted from Knapp et al, 2006 (200 cites)	Not Relevant

S15			The organisation has the necessary power to enforce policy	True/False/Unknown		Adapted from Knapp et al, 2006 (200 cites)	Authority of protector
S16			Information security policy is properly enforced	True/False/Unknown		Adapted from Knapp et al, 2006 (200 cites)	Not Relevant
S17			Trustees clearly understand the ramifications for violating security policies	True/False/Unknown		Adapted from Knapp et al, 2006 (200 cites)	Not Relevant
S18			Policies are consistently enforced across the organization	True/False/Unknown		Adapted from Knapp et al, 2006 (200 cites)	Not Relevant
S19			I feel that if discovered security policy violations are reported to/by the proper authority	True/False/Unknown		Adapted from Knapp et al, 2006 (200 cites)	Authority of protector
S20			Information security rules are enforced by sanctioning the employees who break them	True/False/Unknown		Adapted from Knapp et al, 2006 (200 cites)	Not Relevant

S21	**Culture**		**I feel that the trustee appears to value the importance of security**	**True/False/Unknown**		**Adapted from Knapp et al, 2006 (200 cites)**	**Shared Values**
S22			A culture exists at the organisation that promotes good security practices	True/False/Unknown		Adapted from Knapp et al, 2006 (200 cites)	Not Relevant
S23			Security has traditionally been considered an important organizational value	True/False/Unknown		Adapted from Knapp et al, 2006 (200 cites)	Not Relevant
S24			Good security is the accepted way of doing business in this scenario	True/False/Unknown		Adapted from Knapp et al, 2006 (200 cites)	Not Relevant
S25			The overall environment fosters security-minded thinking	True/False/Unknown		Adapted from Knapp et al, 2006 (200 cites)	Not Relevant
S26			**Information security is a key norm shared by organizational members.**	**True/False/Unknown**		**Adapted from Knapp et al, 2006 (200 cites)**	**Integrity of trustee**

S27	**Surveillance**		Are you aware of being monitored whilst online?	True/False	Surveillance is defined as 'any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered' (Lyon, 2001: 2).	New**; Ball et al,2014	User would not be aware anyway
S28			I feel informed about the type(s) of information that is being gathered during my online usage	5 point scale 1= Not informed to 5=fully informed		New**	Users generally not aware of collected data.
S29		**Data Monitoring**	I feel comfortable that the communications are being monitored	5 point scale 1= very uncomfortable to 5=very comfortable		New**	Not Applicable
S30		**Data Surveillance**	It is necessary for the security services to access messages for public safety reasons.	True/False	**New	New**	Attitude toward external institutions.
S31	**Overall (Abstract)**	**Overall Security**	Overall, I have Confidence in the Security of personal and financial information	True/False		New**	Merge with Counter
S32			(Counter) I feel exposed when I am using personal or financial data online.	True/False	Exposure- Abandoning without shelter or protection.	New**	

Reputation						
Item	**First Order**	**Second Order**	**Item**	**Item Scale**	**Source**	**Inclusion Rationale**
TW1	**Reputation (Collective Measure)**	**Functional Reputation**	Has access to resources	True/False/Unknown	Eisenegger, 2009 ; Josang,2007;Yamagishi,1994; Walsh& Beatty,2007	Not relevant
TW2			Is successful in what they do.	True/False/Unknown		Ability / Domain based
TW3			They know what needs to be done	True/False/Unknown		Comfort/Safety/Care
TW4			The trustee has Specialist knowledge	True/False/Unknown		Not applicable
TW5		**Social Reputation**	The trustee takes our well being seriously	True/False/Unknown		Not applicable
TW6			The trustee knows our needs	True/False/Unknown		c.f hierarchy of needs

Reputation						
Item	**First Order**	**Second Order**	**Item**	**Item Scale**	**Source**	**Inclusion Rationale**
TW7			The trustee takes needs seriously	True/False/Unknown		Duplicate of / Merge with above
TW8			The trustee acts in the interests of customer	True/False/Unknown		Duplicate of TW38/39
TW9			The trustee keeps to promises	True/False/Unknown		May not be known to participant
TW10			The trustee is credible	True/False/Unknown		Not applicable
TW11			The trustee acts to principles	True/False/Unknown		Values driven
TW12			The trustee is a responsible organisation	True/False/Unknown		May not be known to participant
TW12.5			**The trustee has a reputation for being honest**		**Doney & Cannon, 1997**	

Reputation						
Item	**First Order**	**Second Order**	**Item**	**Item Scale**	**Source**	**Inclusion Rationale**
TW13		**Expressive Reputation**	The trustee is likeable	True/False/Unknown		Not applicable online
TW14			The trustee is authentic	True/False/Unknown		Authentic, historical perspective
TW15			The trustee creates a positive impression	True/False/Unknown		
TW16			The trustee has an appealing impression	True/False/Unknown		Not applicable to all scenarios
TW17	**Motivation**	**Extrinsic Motivation**	The trustee is motivated to help me (financially/personally/professionally)	True/False	*New item	Can infer motivation from scenario?
TW18		**Intrinsic Motivation**	Identification with trustee as part of group		Identification. The nine-item scale developed by Hinkle, Taylor, Fox-Cardamone, and Crook (1989) was used to assess identification with	Belongingness and community

Reputation						
Item	**First Order**	**Second Order**	**Item**	**Item Scale**	**Source**	**Inclusion Rationale**
					one's company. Tajfel,1978; Colquitt,2011	
TW19		**Autonomy Support**	The trustee accepts that mistakes I make are part of a learning process		Pelletier, (2013);Tremblay et al (1995, 2009) Sport Motivation Scale. Adapted to motivators for trust.	Not applicable in no choice scenarios
TW20		**Caring**	I feel that the trustee cares about me			Care
TW21		**Structure**	When the trustee asks me to do something, he or she gives me a rationale for doing it			Not applicable
TW22		**Feedback**	The feedback I receive from the trustee is constructive in helping me make improvements			Interaction between parties.
TW23		**Transparency**	The trustee is transparent in his/ her dealings with me	5 point scale: Disagree Strongly to Agree Strongly	**New item	Impossible to know

Reputation						
Item	**First Order**	**Second Order**	**Item**	**Item Scale**	**Source**	**Inclusion Rationale**
TW24	**Integrity**	**Opportunism**	x has a strong sense of justice	5 point scale: Disagree Strongly to Agree Strongly	Meyer et al, 1999	Regulation question
TW25			X will stick to its' word	5 point scale: Disagree Strongly to Agree Strongly	Meyer et al, 1999	Not applicable to all scenarios
TW26			x tries hard to be fair in its dealings with others	5 point scale: Disagree Strongly to Agree Strongly	Meyer et al, 1999	Fairness, out of scope
TW27			I like their values	5 point scale: Disagree Strongly to Agree Strongly	Meyer et al, 1999	Trust not TW
TW28			**sound principles seem to guide their behaviour**	**5 point scale: Disagree Strongly to Agree Strongly**	**Meyer et al, 1999**	**Ethics and opportunism.**

Reputation						
Item	**First Order**	**Second Order**	**Item**	**Item Scale**	**Source**	**Inclusion Rationale**
TW29	**Justice**	**Procedural Justice**	Are you able to express your views during those automated procedures?	5 point scale 1 =to a very small extent to 5 = to a very large extent	Colquitt and Rodell, 2011	All procedural items out of scope
TW30			Can you influence the decisions arrived at by the automated procedures?	5 point scale 1 =to a very small extent to 5 = to a very large extent	Colquitt and Rodell, 2011	All procedural items out of scope
TW31			Are those automated procedures applied consistently?	5 point scale 1 =to a very small extent to 5 = to a very large extent	Colquitt and Rodell, 2011	All procedural items out of scope
TW32			Are the automated procedures free of bias?	5 point scale 1 =to a very small extent to 5 = to a very large extent	Colquitt and Rodell, 2011	All procedural items out of scope
TW33			Are those procedures based on accurate information?	5 point scale 1 =to a very small extent to	Colquitt and Rodell, 2011	All procedural items out of scope

Reputation						
Item	**First Order**	**Second Order**	**Item**	**Item Scale**	**Source**	**Inclusion Rationale**
				5 = to a very large extent		
TW34			Are you able to appeal the decisions arrived at by those procedures?	5 point scale 1 =to a very small extent to 5 = to a very large extent	Colquitt and Rodell, 2011	All procedural items out of scope
TW35			Do those procedures uphold ethical and moral standards?	5 point scale 1 =to a very small extent to 5 = to a very large extent	Colquitt and Rodell, 2011	All procedural items out of scope
TW36	**Overall**		Overall, XX gives the impression of being trustworthy	Yes/No	Battarcherjee, 2002	Assessment of TW by participants
TW37			xxx makes every effort to address my needs	5 point scale: Disagree Strongly to Agree Strongly	Sekhon et al, 2014	Merge with above

Reputation						
Item	**First Order**	**Second Order**	**Item**	**Item Scale**	**Source**	**Inclusion Rationale**
TW38	**Reputation**		**XX has a reputation for looking after its customers**	**5 point scale: Disagree Strongly to Agree Strongly**	**Sekhon et al, 2014**	**Care and Security**
TW39			XX has a reputation for having its customers interests at heart	5 point scale: Disagree Strongly to Agree Strongly	Sekhon et al, 2014	Benevolence

Trust						
Item	**First Order**	**Second Order**	**Item Stem**	**Item Scale**	**Source**	**Inclusion Rationale**
T1	**Belief**	**Confidence**	**XX would be trustworthy in information handling.**	**Seven-point scales anchored with "strongly disagree" and "strongly agree"**	**Malhotra (2004) IUIPC - adapted**	**Reworded to I know that my information is safe and access is limited only to authorised personnel.TW-->Trust**

Trust						
Item	**First Order**	**Second Order**	**Item Stem**	**Item Scale**	**Source**	**Inclusion Rationale**
T2			XX would tell the truth and fulfill promises related to the information provided by me.	Seven-point scales anchored with “strongly disagree” and “strongly agree”	Malhotra (2004) IUIPC - adapted	Unrelated to belief
T3			I trust that XX would keep my best interests in mind when dealing with information.	Seven-point scales anchored with “strongly disagree” and “strongly agree”	Malhotra (2004) IUIPC – adapted	Benevolence
T4			XX are in general predictable and consistent regarding the usage of the information.	Seven-point scales anchored with “strongly disagree” and “strongly agree”	Malhotra (2004) IUIPC – adapted	More to do with ability and cognitive
T5			XX are always honest with customers when it comes to using the information that I would provide.	Seven-point scales anchored with “strongly disagree” and “strongly agree”	Malhotra (2004) IUIPC – adapted	Merged to T7, include perception.
T6		**Communication**	I am confident in the cybersecurity threat safeguards offered by XX	5 point scale 1=Not Confident to 5= very Confident	**New	Security

Trust

Item	First Order	Second Order	Item Stem	Item Scale	Source	Inclusion Rationale
T7			**I believe that the information privacy assurances offered by XX will be honoured.**	**5 point scale 1=No Belief in Trustee to 5= Strong Belief in Trustee**	****New**	**Perception of honesty. Privacy-> Trust**
T8			I believe that being associated with XX reduces the uncertainty I face	5 point scale 1=No uncertainty to 5=Uncertain	Morgan & Hunt, 1996. Confident Expectations	Uncertainty attenuation
T9		**Commitment**	I believe that XX is committed to my well being	5 point scale 1=Not committed to 5=Committed	Morgan & Hunt, 1996	Commitment to the relationship is defined as an enduring desire to maintain a valued relationship
T10		**Co-operation**	XX is willing to cooperate to get tasks done.	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Morgan & Hunt, 1996 - Willingness to act.	Not applicable
T11	**Affective Trust**		I would be willing to let x have complete control over.	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Meyer et al, 1999 – modified	Belief and Care
T12			I really wish I had a good way to keep an eye on x	5 point scale 1=Disagree Strongly to 5= Agree Strongly		Monitoring=Behaviour/Delegation

Trust

Item	First Order	Second Order	Item Stem	Item Scale	Source	Inclusion Rationale
T13			I would be comfortable giving X a task or problem which was critical to me, even if I could not monitor their actions.	5 point scale 1=Disagree Strongly to 5= Agree Strongly		Monitoring=Behaviour/Delegation
T14		**Subjectivity**	X considers me as an individual	5 point scale from individual to Xx	Malone(2012); Mahar et al (2012) - conceptualising belongingness; Maslow(1943)	Valued Client/Customer
T15		**Inclusion**	I feel valued and 'fit in' (included).	5 point Scale from valued to excluded		Belongingness
T16		**Reciprocity**	I feel that I belong to a community	5 point Scale from 1= feel part of the Trustees community to 5= Do not feel part of the community.		Merge with T15, sense of belonging.
T17		**Groundedness**	My sense of belonging is shared with others.	5 point scale from 1=feel that I belong with other trustors to 5= Do not feel I belong with other trustors.	Grounded to external referent.	Belongingness

Trust						
Item	**First Order**	**Second Order**	**Item Stem**	**Item Scale**	**Source**	**Inclusion Rationale**
T18		**Dynamism**	Flexibility with current and previous situations	5 point scale 1= inflexible relationship to 5= fully flexible relationship		Scenario dictates the flexibility
T19		**Self-Determination**	Choice in belonging or participating in the group	Choice/No Choice		Merge with T15, sense of belonging.
T21			I have a preference towards 1. Trusting others with whom I have experience, OR 2. I rely more on possibilities and risk taking in online situations OR 3. I analyse situations logically and objectively before acting	Sensing/Intuition/Thinking preference	Mallach(2000),Myers(2003) Mayer et al (1999) -modified	Trust Propensity
T22			Most experts tell the truth about the limits of their knowledge	5 point scale 1=Disagree Strongly to 5= Agree Strongly		Ability / Behaviour
T23			One should be very cautious with strangers	5 point scale 1=Disagree Strongly to 5= Agree Strongly		Not applicable

Trust						
Item	**First Order**	**Second Order**	**Item Stem**	**Item Scale**	**Source**	**Inclusion Rationale**
T24			Most people can be counted on to do the things they say they will do	5 point scale 1=Disagree Strongly to 5= Agree Strongly		Co-variates
T25			These days, you must be alert or someone is likely to take advantage of you	5 point scale 1=Disagree Strongly to 5= Agree Strongly		As Above, propensity question not trust
T26			Most salespeople are honest about describing their products	5 point scale 1=Disagree Strongly to 5= Agree Strongly		Not relationship based.
T27			Most people will not overcharge those who are ignorant of their speciality	5 point scale 1=Disagree Strongly to 5= Agree Strongly		Not applicable for modern online
T28	**Salient Values**	**Values**	Same values – different values	5 point scale 1=Different Values to 5= Same Values	Siegrist et al,2000;Earle & Cvetovich (2000); Morgan & Hunt (1996)	Value Salience
T29			Same goals – different goals	5 point scale 1=Different Goals to 5= Same Goals		Not able to assess goals of the organisation

Trust

Item	First Order	Second Order	Item Stem	Item Scale	Source	Inclusion Rationale
T30			Acts as I would – acts different than I would	5 point scale 1=Acts as I would to 5= Acts differently to me	Siegrist et al,2000	Would a person act the same as their trustee?
T31			Thinks like me – thinks unlike me	5 point scale 1=Thinks like me to 5= Thinks unlike me		Impossible to rate
T32			Same opinions – different opinions	5 point scale 1=Opinions like me to 5= Different opinions to me		We all have different and varying opinions.
T33		**Social Trust**	Acts Responsibly	5 point scale 1=Does not act responsibly toward me to 5= Acts very responsibly towards me		Responsibility of trustee in scenarios
T34			Bothered about the consequences of trusted actions			Can't always know consequences
T35	**Overall**	**Overall trust**	I believe that I can trust the other party.	5 point scale 1=Disagree Strongly to 5= Agree Strongly	New - Compound measure	Measure of overall belief

Trust						
Item	**First Order**	**Second Order**	**Item Stem**	**Item Scale**	**Source**	**Inclusion Rationale**
T36	**Affective Trust**		XX is always honest with me	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Doney & Cannon, 1997	Honesty increases trust
T37			XX is concerned about my best interests	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Sekhon et al, 2014	Trustworthiness
T38			XX makes every effort to address my needs	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Sekhon et al, 2014	Caring attitude
T39	**Benevolence**		XX Shows respect for the customer	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Sekhon et al, 2014	Caring attitude
T40			Does whatever it takes to make me happy	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Sekhon et al, 2014; Hess,1995	Not always true for all trustors
T41			Acts in the best interests of customers	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Sekhon et al, 2014; Sirdeshmukh et al, 2002	Trustworthiness

Trust						
Item	**First Order**	**Second Order**	**Item Stem**	**Item Scale**	**Source**	**Inclusion Rationale**
T42			Can be relied on to give honest advice	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Sekhon et al, 2014; Sirdeshmukh et al, 2002	Duplicate of T36

OUTCOMES						
Item	**First Order**	**Second Order**	**Item Stem**	**Item Scale**	**Source**	**Inclusion Rationale**
O1	**Achievement**	**Proximal/ End Goal**	I was able to achieve my goal		True/False	Success Indicator informs the analysis of fulfilled desire.
O2			Achieving the transaction gave me the confidence to engage with the trustee again		5 Point Likert Scale. Very Unlikely to Very Likely	Confidence (Trust Belief)

OUTCOMES

Item	First Order	Second Order	Item Stem	Item Scale	Source	Inclusion Rationale
O3			I can assess how the organisation helps others to meet their goals.		5 Point Likert Scale. Very Unlikely to Very Likely	Trustworthiness Indicator
O4		**Desired Change**	I was able to assess the before and after state of the transaction with confidence		True/False	Transparency
O5			My opinion of the trustee has increased based on our history of transactions		5 Point Likert Scale. Not Increased At All to Increased Greatly	Trust Belief
O6			The trustee has informed me of other customers that have seen positive outcomes from their association.		5 Point Likert Scale. Not informed to Fully Informed	Trustworthiness Indicator
O7		**Results**	The most recent transaction between myself and the trustee was successful.		True/ False	Duplicate of O1
O8			I am able to know how the association between myself and the trustee has benefitted me.		5 Point Likert Scale. Fully Visible to Not Ascertainable	Trust Belief

OUTCOMES

Item	First Order	Second Order	Item Stem	Item Scale	Source	Inclusion Rationale
O9			I am able to assess how the trustee dealt with situations similar to mine.		5 Point Likert Scale. Fully Visible to Not Ascertainable	Trustworthiness Indicator
O10	**Audience**	**Security**	I am confident that my transaction details are kept from other parties.		5 point Likert scale. Very Confident to not confident.	Part of Vulnerability
O11			I am confident that only myself and the trustee and authorised parties can see our history of interactions		5 point Likert scale. Very Confident to not confident.	Part of Privacy
O12			I am unable to see the transactions carried out by other customers.		True/False	Part of Security
O13	**Feedback**	**Assessment**	**I am able to give objective feedback to the service provider**		**True/False**	**Communication (TW)**
O14		**Side Effects**	There are no implications to the association that I am wary of.			User would not know implications of recent ops.

OUTCOMES

Item	First Order	Second Order	Item Stem	Item Scale	Source	Inclusion Rationale
O15		**Expectation Met**	The results of the interaction between myself and the service provider met my expectations.			Too Marketing-y
O16	**Benevolence**	**Empathy**	x is very concerned about my welfare	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Meyer et al, 1999 – modified	Not applicable to online
O17			My needs and desires are important to x	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Meyer et al, 1999 – modified	Not applicable in all scenarios
O18			X would not knowingly do anything to harm me	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Meyer et al, 1999 – modified	Benevolence & Safety
O19			XX really looks out for what is important to me.	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Colquitt & Rodell, 2011	Not applicable in all scenarios

OUTCOMES

Item	First Order	Second Order	Item Stem	Item Scale	Source	Inclusion Rationale
O20			XX will go out of his/her way to help me	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Colquitt & Rodell, 2011	Not applicable online
O21			XX is open and receptive to customer needs.	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Battarcherjee, 2002	Not applicable online
O22			XX keeps its customers' best interest in mind during most transactions.	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Battarcherjee, 2002	Same as O23
O23			XX makes good-faith efforts to address most customer concerns.			Benevolence & feedback

DELEGATION

Item	First Order	Second Order	Item Stem	Item Scale	Source	Inclusion Rationale
D1	**Ability**	Competence/ predictability	I feel that the agent is capable/ I feel that the outcome of the interaction is predictable.		Schoorman, 2016 ;Castelfranchi,2001	Competance
D2		Reliance	I am reliant on passing my details to the agent in order to complete the task	Reliant/ Not Reliant/ Direct reliance on trustee		Importance measure
D3		Belief	My confidence in the agent is based on:	Previous Experience / Similar Experience/Reasoning/ Reputation	**New	Belief--> Action
D4	**Delegation Type**	Strong/ weak	I am /am not aware that the information is being dealt with by an external agent.	Am/ am not/I choose/ unknown	Castelfranchi, 2001	Transparency
D5		Disposition	The agent is disposed to do what I want it to do		Castelfranchi, 2001	Related to motivation of Trustee?
D6		Dependence	I need to delegate the task in order to do it.	Need/Depend/Rely	Castelfranchi,2001	Same as D2

DELEGATION

Item	First Order	Second Order	Item Stem	Item Scale	Source	Inclusion Rationale
D7	**Intention**	Expectation	I believe that delegating the task will achieve my task goal	5 point scale of belief in success 1=slim, 5=confident	Castelfranchi,2001	Confident expectation
D8		Willingness	The agent is willing to act on my behalf		Castelfranchi,2001	Related to motivation of Trustee?
D9		Authority	I have the final say in whether a task is delegated to a third party.	5 point scale 1=Disagree Strongly to 5= Agree Strongly	**New	Usually no choice, trustee has authority.
D10		Consent	I have explicitly consented to the trustee using my credentials to act on my behalf	5 point scale 1=Disagree Strongly to 5= Agree Strongly	**New	Many ssituations is implicit in contract of services.
D11		Cognitive Trust	I feel that I can trust the delegated agent to act in my place.	5 point scale 1=Disagree Strongly to 5= Agree Strongly	**New	Trust--> Action
D11.5			I feel that the task is delegated to a trustworthy agent.	5 point scale 1=Disagree Strongly to 5= Agree Strongly		TW--> Action.Bypassing the belief step.

DELEGATION

Item	First Order	Second Order	Item Stem	Item Scale	Source	Inclusion Rationale
D12		Transitive Trust	I trust the trustee enough to allow him/ her to delegate the task to another person/ Information System	5 point scale 1=Disagree Strongly to 5= Agree Strongly	**New	The Trust--> Action is transitive to other parties.
D13			I have trust in the third party to carry out the instructions correctly	5 point scale 1=Disagree Strongly to 5= Agree Strongly	**New	Covered by D13
D14			The trusted third party will not disseminate my details beyond the trustees and myself.	5 point scale 1=Disagree Strongly to 5= Agree Strongly	**New	Not known by participant, trust belief question.
D15			I feel secure inputting my details into a third party application in order to carry out the task.	5 point scale 1=Disagree Strongly to 5= Agree Strongly	**New	Not applicable
D16	**Performance**	Fulfillment	It is easy to evaluate the delegates skills accurately	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Meyer et al, 1999 - modified	Feedback to participant, communication.

DELEGATION

Item	First Order	Second Order	Item Stem	Item Scale	Source	Inclusion Rationale
D17			How much work is done is important in reviewing performance	5 point scale 1=Disagree Strongly to 5= Agree Strongly		Covered by D16 above.
D18			How much effort the delegate put into the task is important	5 point scale 1=Disagree Strongly to 5= Agree Strongly		Not relevant
D19			Trustee has substantial leeway in determining how they accomplished the final deliverable.	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Mayer et al, 2005	Related to the weak/strong delegation constraints.
D20			Trustee has a great deal of autonomy on this task.	5 point scale 1=Disagree Strongly to 5= Agree Strongly		More autonomy proportional to level of trust?
D21			Trustor allowed the trustee to have control over this task.	5 point scale 1=Disagree Strongly to 5= Agree Strongly		By defintion trustee has control.
D22			The trustee closely monitored potential problems encountered by the delegated agent.	5 point scale 1=Disagree Strongly to 5= Agree Strongly		Authority of Trustee

DELEGATION						
Item	**First Order**	**Second Order**	**Item Stem**	**Item Scale**	**Source**	**Inclusion Rationale**
D23			The trustee tried to keep a close eye on the delegated agent	5 point scale 1=Disagree Strongly to 5= Agree Strongly		Covered by D22
D24			I trust the delegated agent to do what it/he/she says they will do	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Sekhon et al, 2014	May not be the choice of the participant.
D25			I trust XX to have my best interests at heart	5 point scale 1=Disagree Strongly to 5= Agree Strongly	Sekhon et al, 2014	Does the benevolence extend transitively as the delegate may work for many clients.

Appendix A2: Sample questionnaire in word format

Cybersecurity in Online Banking questionnaire

PARTICIPANT INFORMATION STATEMENT

The aim of this study is to investigate the roles of security, privacy, protection and trust formation in online environments. The study is being conducted by Duncan Greaves at Coventry University.

You have been selected to take part in this questionnaire survey because you have experience in this area. Your participation in the survey is entirely voluntary, and you can opt out at any stage by closing and exiting the browser. If you are happy to take part, please answer the following questions relating to cybersecurity in online banking situations.

Your answers will help us to link your responses to the project aims. The survey should take approximately 10 minutes to complete. Your answers will be treated confidentially and the information you provide will be kept anonymous in any research outputs/publications.

Your data will be held securely on protected computer files held at Coventry University. All data will be deleted by 31/12/2020. The project has been reviewed and approved through the formal Research Ethics procedure at Coventry University. For further information, or if you have any queries, please contact the lead researcher Duncan Greaves, greavesd@uni.coventry.ac.uk. If you have any concerns that cannot be resolved through the lead researcher, please contact Dr Alexeis Garcia Perez. Research Supervisor, Coventry University, Coventry, UK CV1 5FB, email: ab1258@coventry.ac.uk. Thank you for taking the time to participate in this survey. Your help is very much appreciated.

I have read and understood the above information. I understand that, because my answers will be fully anonymised, it will not be possible to withdraw them from the study once I have completed the survey. I agree to take part in this questionnaire survey. I confirm that I am aged 18 or over.

☐Yes	☐No

Questionnaire Scenario

This questionnaire seeks responses about attitudes to using an online banking platform that you have had transactions with ***more than once.***

Think back to your most recent interaction with the online bank (For example, bill payment, balance enquiry, transfer) and answer the following questions relating to your experience.

The aim is to answer as truthfully as you are able, without thinking too long about any individual answer. Please answer all of the questions.

I use / have used online banking before

☐Yes	☐No

Participant Background Information

1. Which area do you currently live in?

☐UK(excluding Europe)	☐North America
☐Europe (excluding UK)	☐South America
☐ South Asia (India, Pakistan, Bangladesh)	☐Africa
☐Middle East	☐Other (Please Specify):

2. Your Age Group:

☐Under 25	☐45-54
☐25-34	☐55-64
☐35-44	☐Over 65

3. Your Gender:

☐Female	☐Male

4. Your level of education (Choose one):

☐None	☐College study, not degree level
☐Some schooling	☐Degree Level
☐Finished school	☐Postgraduate Level

5. How much have you heard or read during the last year about the use and potential misuse of the information collected from the Internet? (Choose one)

☐Not a lot	☐A little	☐Quite a lot	☐Very much

6. I have a preference towards (Please choose one):

☐Trusting others with whom I have experience
☐I rely more on possibilities and risk taking in online situations
☐I analyse situations logically and objectively before acting

7. Compared to others, I am more sensitive about the way online companies handle my personal information (Choose one).

☐Strongly disagree	☐Disagree	☐Neither agree nor disagree	☐Agree	☐Strongly agree

8. I generally trust other people

☐Yes	☐No

9. I generally have faith in humanity

☐Yes	☐No

Based on the scenario, please rate how strongly you disagree or agree with the following statements

	Strongly Disagree	**Disagree**	**Neither agree nor disagree**	**Agree**	**Strongly Agree**
1. The bank appears to value the importance of security.	☐	☐	☐	☐	☐
2. The bank has a reputation for being honest.	☐	☐	☐	☐	☐
3. The bank should not use personal information for any purpose unless I have authorised it to do so.	☐	☐	☐	☐	☐
4. I trust the bank enough to allow it to delegate the task of fulfilling my instructions to another person or information system (e.g. payment processing, call centre).	☐	☐	☐	☐	☐
5. I believe that if the bank delegated tasks (e.g. payment processing) it was to help achieve my transaction goal.	☐	☐	☐	☐	☐
6. I am able to assess how the bank dealt with situations similar to mine.	☐	☐	☐	☐	☐
7. The information I receive from the bank is constructive in helping me manage my finances. (e.g. products and savings options).	☐	☐	☐	☐	☐
8. The bank would not knowingly do anything to harm me.	☐	☐	☐	☐	☐
9. Information security is a key normal behaviour of the bank.	☐	☐	☐	☐	☐
10. It concerns me when I see my personal preferences used in targeted advertising by the bank without my consent.	☐	☐	☐	☐	☐
11. The bank has specialised capabilities that can increase my financial wellbeing.	☐	☐	☐	☐	☐
12. I am aware when the information that I give to the bank is being dealt with by an external agent (e.g. Credit checking, payment processing).	☐	☐	☐	☐	☐

Based on the scenario, please rate how strongly you disagree or agree with the following statements

	Strongly Disagree	**Disagree**	**Neither agree nor disagree**	**Agree**	**Strongly Agree**
13. Sound principles seem to guide the behaviour of the bank.	☐	☐	☐	☐	☐
14. My opinion of the bank has increased based on our history of transactions.	☐	☐	☐	☐	☐
15. The bank has informed me of other customers that have seen positive outcomes from their association (e.g. customer stories, feedback scores).	☐	☐	☐	☐	☐
16. Achieving the online transaction gave me the confidence to engage with the bank again.	☐	☐	☐	☐	☐
17. I can trust the bank or their agent to act in my place.	☐	☐	☐	☐	☐
18. I know that my information is safe and access is limited only to authorised personnel.	☐	☐	☐	☐	☐
19. The bank knows what needs to be done.	☐	☐	☐	☐	☐
20. The bank should protect my assets and information from cyberthreats and their effects.	☐	☐	☐	☐	☐
21. The bank should protect our relationship from cyberthreats and their effects.	☐	☐	☐	☐	☐
22. The bank keeps my best interests at heart when dealing with information.	☐	☐	☐	☐	☐
23. I am able to give objective feedback to the bank or their service provider.	☐	☐	☐	☐	☐
24. The bank or their agent have a great deal of autonomy over fulfilling their tasks.	☐	☐	☐	☐	☐

Based on the scenario, please rate how strongly you disagree or agree with the following statements

	Strongly Disagree	**Disagree**	**Neither agree nor disagree**	**Agree**	**Strongly Agree**
25. The bank makes rules about our interactions, sets limits to activities and enforces the rules and limits to our interaction.	☐	☐	☐	☐	☐
26. Information I have given to the bank in one context should not be used in an unrelated context without my permission or knowledge.	☐	☐	☐	☐	☐
27. The bank has access to resources that I do not.	☐	☐	☐	☐	☐
28. The bank has a reputation for looking after its customers.	☐	☐	☐	☐	☐
29. The bank has the skills and experience to perform transactions in an expected manner.	☐	☐	☐	☐	☐
30. If the banking transaction does not work I have sufficient assets or alternatives to cover any loss.	☐	☐	☐	☐	☐
31. Data privacy is more important to me than data sharing.	☐	☐	☐	☐	☐
32. I am unable to influence the presence of threats inherent in doing the task online.	☐	☐	☐	☐	☐
33. The bank is very capable of performing the job.	☐	☐	☐	☐	☐
34. I believe that the information privacy assurances offered by the bank will be honoured.	☐	☐	☐	☐	☐

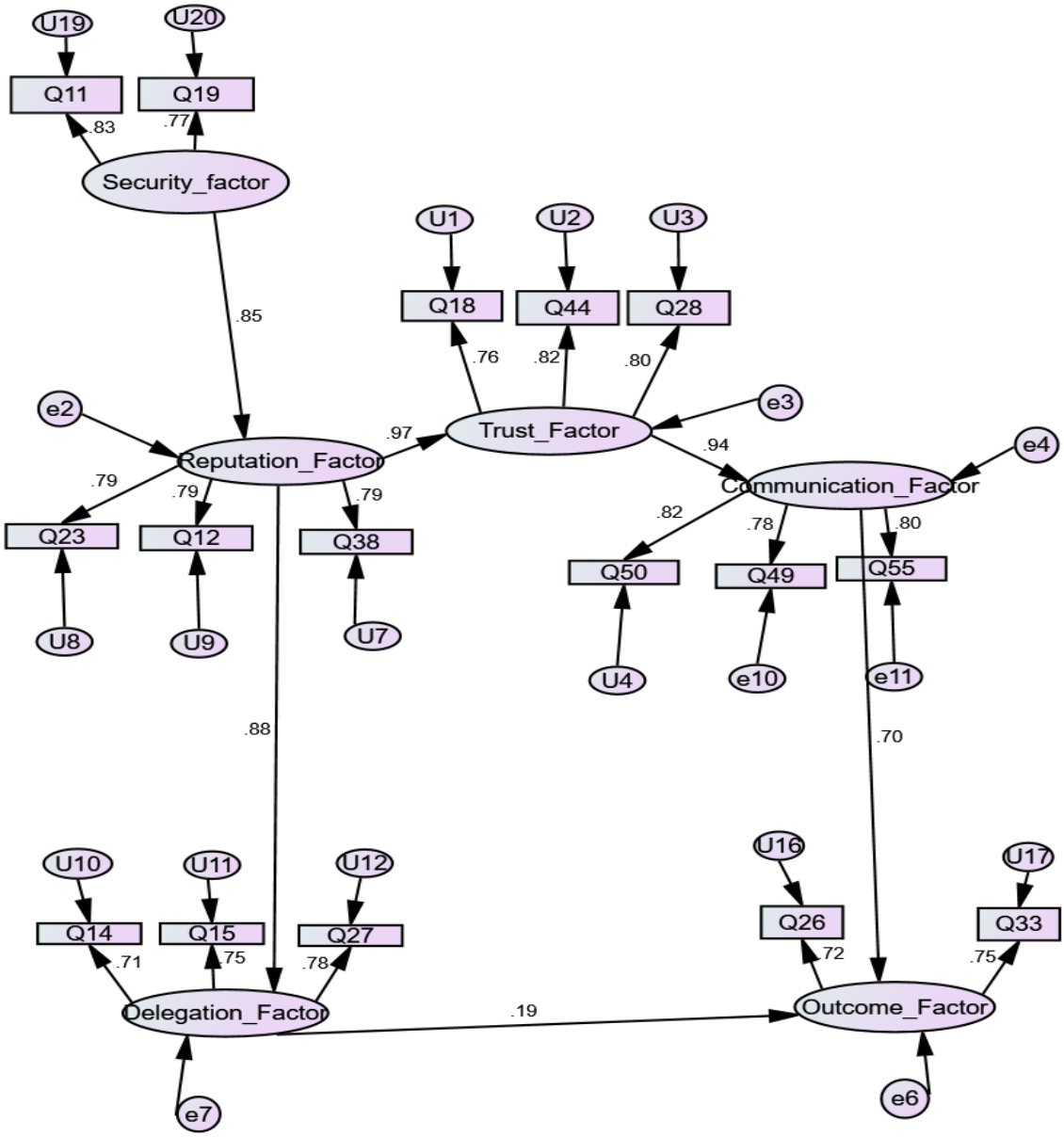
Based on the scenario, please rate how strongly you disagree or agree with the following statements:

	Strongly Disagree	**Disagree**	**Neither agree nor disagree**	**Agree**	**Strongly Agree**
35. I have the possibility of redress (remedy or refund) in the event of task failure due to cyber threat.	☐	☐	☐	☐	☐
36. I am able to understand the potential cyber threats and risks fully with online banking transactions.	☐	☐	☐	☐	☐
37. I feel that my connectedness to the bank protects me from the transaction risk.	☐	☐	☐	☐	☐
38. I have confidence that my information is not modified without consent and is destroyed after use, or at my request.	☐	☐	☐	☐	☐

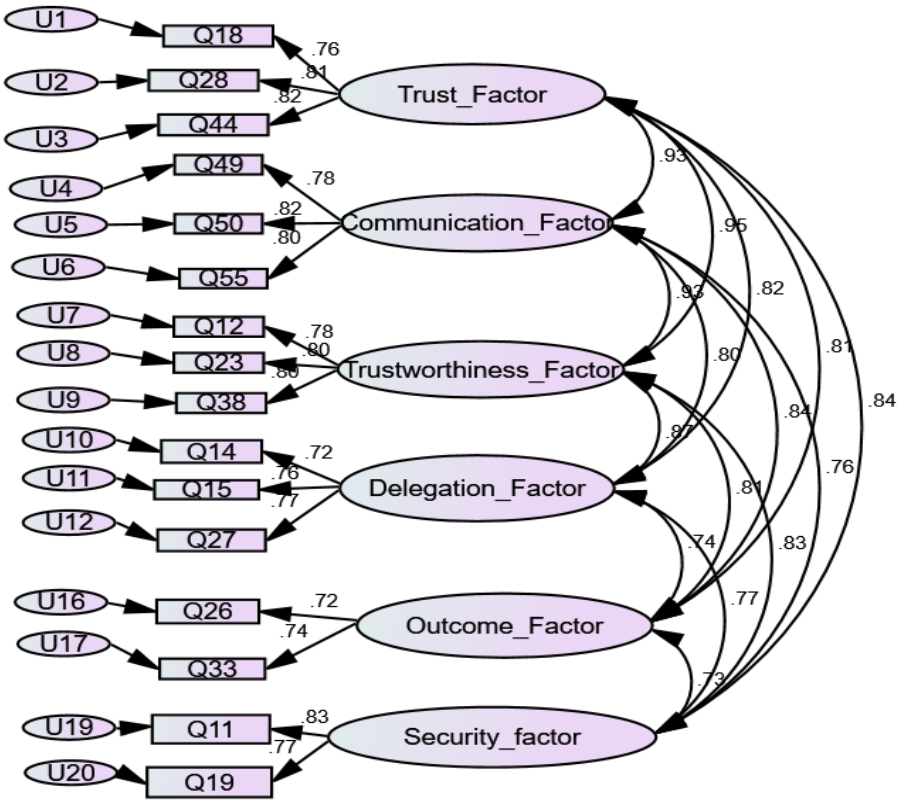
Thank you for your participation in this survey.

Appendix A3: AMOS SEM Modelling Output

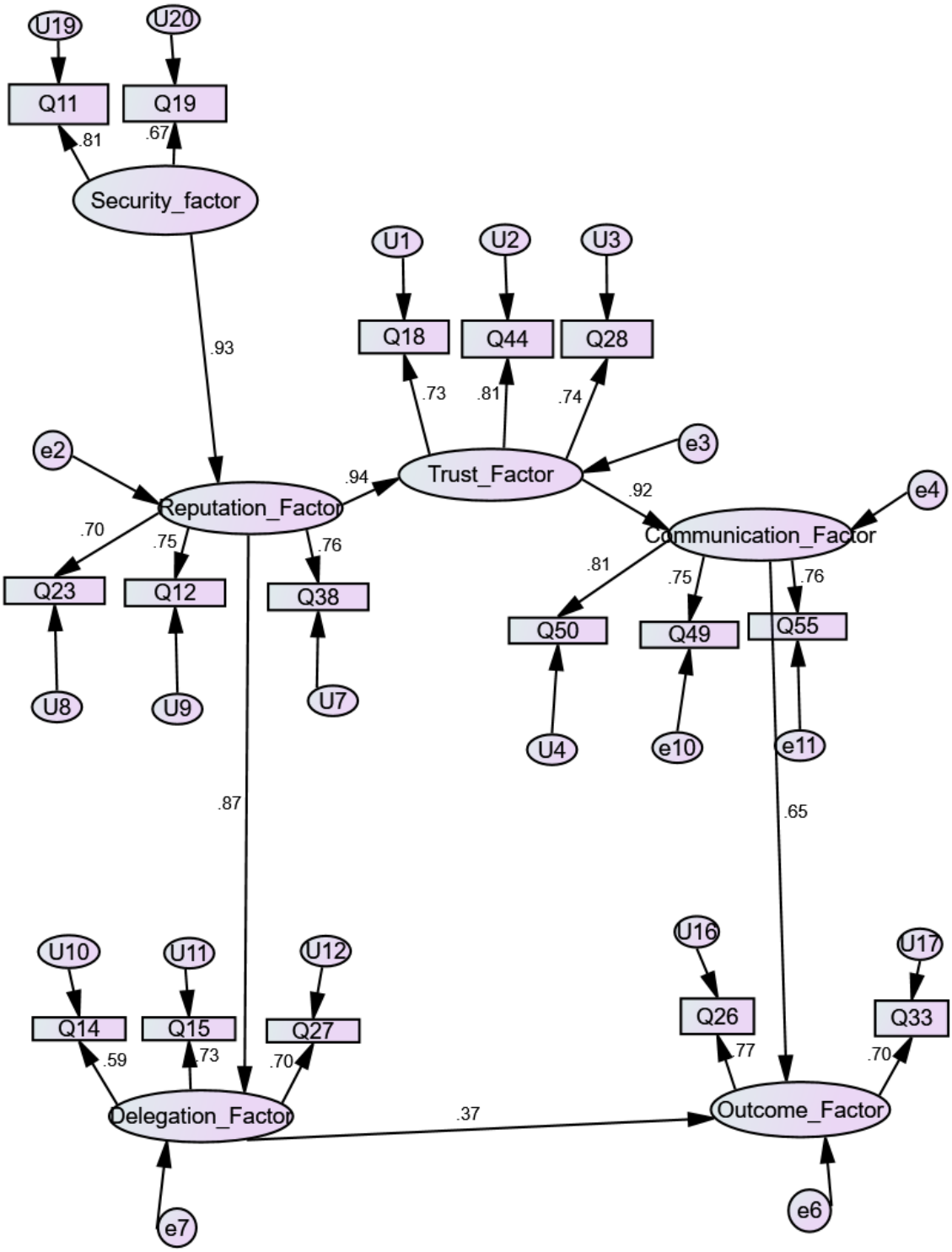
SEM Model Final



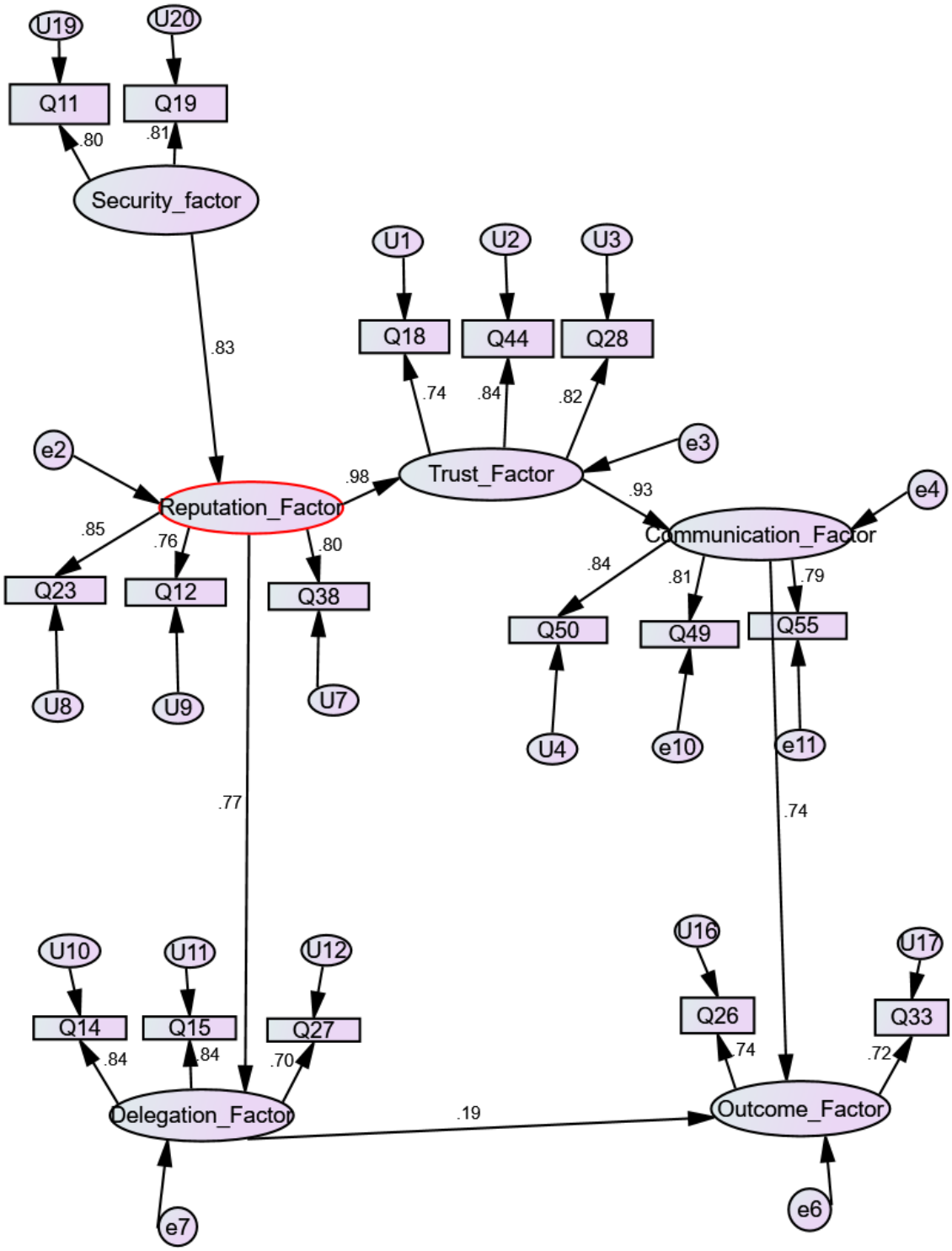
CFA Model Final



Scenario 1: SEM Model Retail



Scenario 2: Model Banking



Scenario 3: Model Healthcare