Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: an intellectual capital perspective

Garcia-Perez, A., Sallos, M. & Tiwasing, P.

Original citation & hyperlink:
Garcia-Perez, A, Sallos, M & Tiwasing, P 2021, 'Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: an intellectual capital perspective', Journal of Intellectual Capital, vol. (In-press), pp. (In-press).
https://dx.doi.org/10.1108/JIC-06-2021-0166

DOI 10.1108/JIC-06-2021-0166
ISSN 1469-1930

Publisher: Emerald

Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: an intellectual capital perspective

Alexeis Garcia-Perez[a], Mark P. Sallos[b] and Pattanapong Tiwasing[c]
a. Professor of Management Information Systems. Centre for Business in Society, Coventry University, Priory Street, Coventry, CV1 5FB, United Kingdom.
Visiting Research Scholar, Knowledge Management. Georgetown University, 3700 O St NW, Washington, DC 20057, United States.
Corresponding author.
Email: alexeis.garcia-perez@coventry.ac.uk.

b. Lecturer in Business Analytics. Higher Colleges of Technology, Dubai, Academic City, United Arab Emirates.
Email: msallos@hct.ac.ae

c. Research Fellow in Quantitative Research Methods. Centre for Business in Society, Coventry University, Priory Street, Coventry, CV1 5FB, United Kingdom.
Email: pattanapong.tiwasing@coventry.ac.uk

Abstract

Purpose:
This research addresses the relationships between the current, dynamic organisational cyber risk climate, organisational cybersecurity performance and changes in cybersecurity investments, with an aim to address the hostile epistemic climate for intellectual capital management presented by the dynamics of cybersecurity as a phenomenon.

Design/methodology/approach:
Expanding on the views of digital security and resilience as a knowledge problem, the research looks at cybersecurity as a critical capability within organisations, particularly relevant in critical infrastructure sectors. The problem is studied from the perspective of 400 C-level executives from critical infrastructure sectors across the UK. Data collected at the peak of the COVID-19 pandemic, a time when critical infrastructure organisations have been under a significant strain due to an increase in cybersecurity incidents, was analysed using Partial Least Square Structural Equation Modelling.

Findings:
The research found a significant correlation between the board's perception of a change in their cybersecurity risk climate and patterns of both the development of cybersecurity management capabilities and cybersecurity investments. We also found that a positive

correlation exists between the efforts placed by critical infrastructure organisations in cybersecurity training and the changes in investment in their cybersecurity, particularly in relation to their intellectual capital development efforts.

Originality:
To the best of our knowledge, this is the first paper that explores the board's perception of cybersecurity in critical infrastructure organisations both from the intellectual capital perspective and in the dynamic cyber risk climate derived from the COVID-19 crisis. Our findings expand on the growing perception of cybersecurity as a knowledge problem, and thus inform future research and practice in the domain of intellectual capital management and its role in supporting the cybersecurity and digital resilience of business and society.

Keywords
Cybersecurity capabilities; cyber crisis response; cybersecurity performance; digital resilience; COVID-19.

Acknowledgements:
This research was conducted with funding awarded by Coventry University in 2020 for the study of the digital resilience of organisations from UK critical infrastructure sectors to inform cybersecurity management policies.

1. Introduction

The growing integration of Internet-connected technology in organisations of all types critical infrastructure organisations has generated a paradoxical dynamic in the current socio-economic environment: organisations need to balance their efforts to adopt new technologies and their applications while managing the risks associated to the digital environment (Alcaraz and Zeadally, 2015). This is particularly true for organisations from sectors in which the socio-economic security and the public health or safety of a country relies upon.

The first part of this dynamic reflects efforts by organisations to give their core systems and structures a 'smart' dimension in order to increase their accessibility and efficiency, and to expand their functionality. The second part deals with the effects of this integration on the likelihood and potential impact of the misuse and failure of technologies as a result of cybersecurity incidents. Such incidents can be a substantial threat to an organisation's intellectual capital, its sustainability, and its competitive performance (Renaud *et al.,* 2019). In recognition of this, an emerging body of work within Intellectual Capital research addresses the protection of informational assets as a complex knowledge problem that extents from the workforce through to the executive level in organisations (Dabic *et al.,* 2020, Renaud *et al.,* 2019, Sallos *et al.,* 2019). Authors such as Disparte and Furlow (2017) have gone one step further to argue that the best investment an organisation can make in its cybersecurity is the provision of better training for its workforce. In this sense, He *et al.* (2019) have concluded that organisations can benefit by integrating a cybersecurity awareness training program into their strategic management of intellectual capital and organisational knowledge, while Al-Awadi and Renaud (2007) have referred to awareness training as a key factor for the successful implementation of information security in organisations.

This paper adds to the current understanding of what drives executives and senior managers in critical infrastructure sectors to invest in their intellectual capital and therefore improve their organisations' ability to (1) react quickly and effectively to cyber incidents, and (2) effectively adapt to an increased activity in the digital space, where cyber criminals conduct malicious activity potentially affecting their operations.

1.1. Cyber, risks and critical infrastructure organisations

While historically seen as a primarily technical problem, organisational cybersecurity and cyber risk management are increasingly viewed through a wider lens which also often includes organisational, legal and knowledge management measures. Once integrated into an organisation –as a complex socio-technical system, risks that were previously technical, well defined and containable inherit new properties derived from their new context and its actors: people (Noguchi and Ueda, 2017). Such properties imply interdependencies and connections between risks, as well as the emergence of new risks. They limit the organisation's ability to analyse, classify and understand the cyber risks, especially as they interact with other domains of risk such as financial, ethical, health and/or safety, or even social risks. (Sun *et al*., 2006; Sallos *et al.,* 2019). The resulting complexity highlights the importance of further understanding how critical infrastructure organisations perceive, govern and manage cyber risk, especially when faced with external pressures, disruptions, or abnormal circumstances. In particular, it is important to better understand the relationship between the cost associated to developing the intellectual capital of the organisation and that of recovering from a cybersecurity incident as economists increasingly classify both cybersecurity and intellectual capital as true capital costs.

In the context of the coronavirus COVID-19 pandemic, critical infrastructure organisations have proven to be under distinct tension in many respects, which has led to a better understanding of their need for more solid cyber defences. For instance, healthcare systems rely on the integrity and accessibility of their information and communication technologies (ICT) infrastructure to deal with the unavoidable spikes in demand. In a pandemic, the resources available to mitigate and respond to cyber-attacks are limited, while even a small system failure can cause loss of life (O'Neill, 2020). Thus, despite the clear difference between the two, a manifested risk such as a widespread infectious disease affects the likelihood and impacts of cybersecurity disruptions or failures, often described as the cyber risk climate (Wagner and Disparte, 2016). To define the cyber risk climate, we build on the notion of "systemic financial risk" purposed by the Group of Ten (2001) and the definition of "system cyber risk" introduced by World Economic Forum (2016) as "*Systemic cyber risk is the risk that a cyber event (attack(s) or other adverse event(s)) at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic*

security or national security". Throughout the paper, the notion of cyber risk climate will thus be used to denote the systemic cyber risk conditions faced by organisations; particularly, it will be used to highlight aggregate shifts in vulnerability and threat patterns (further clarified in section 2.1).

At the same time, cyber criminals can speculate the disruption and structural changes following the society's response to a pandemic in order to develop new targets or new the ways to attack existing systems (Zaboeva and Frydrych, 2020, Newman 2020, Brown 2020, Wiggen 2020). As a result, the hostility of the cyber risk climate faced by organisations has been amplified by developments in a seemingly distinct and independent domain of risk: infectious diseases. This also highlights how, given a societal reliance on critical infrastructures in order to absorb and overcome disruptions, the importance of cybersecurity in such organisations is particularly notable in times of crisis.
In this context, this paper seeks to explore how critical infrastructure organisations respond to a change in their cyber risk climate, based on how members of their management boards assess key indicators of their cybersecurity performance. This objective is relevant for two main reasons. Firstly, we aim to understand and document how critical infrastructure organisations have perceived and responded to cyber risks in the context of the COVID-19 pandemic, when investments in intellectual capital –e.g. cybersecurity training, may not have been prioritised over more pressing issues. To the best of our knowledge, this is the first paper that explores the board's perception of cybersecurity in critical infrastructure organisations in the dynamic cyber risk climate derived from the COVID-19 crisis. Secondly, the research addresses a gap in the current literature by identifying elements that influence the perception of management about the cybersecurity of their organisation when there are changes in their cyber risk climate. In this sense, we seek to identify indicators of cybersecurity that could help change the perception of cybersecurity in the management board in critical infrastructure organisations, and thus lead to more effective responses to changes in their risk climate.

This narrative is primarily based on two operating assumptions, as follows: (1) the COVID-19 pandemic has aggravated the cyber risk climate, and (2) there is a need for a better understanding of how critical infrastructure organisations respond to the increase in the potential scope and impact of cyberattacks. These assumptions are explored in section 2 of this paper, given their relevance to the hypotheses upon which this research is founded.

Section 3 of the paper describes the methodological approach of the study, with a focus on how data was collected from C-level executives in critical infrastructure sectors in the UK and the analysis of the data using Partial Least Square Structural Equation Modelling (PLS-SEM). The results of the analysis are presented and analysed in sections 4 and 5 respectively, followed by the conclusions of the study in section 6.

2. Theory development

2.1. Why critical infrastructure? COVID-19 and the cyber risk climate

The COVID-19 pandemic has aggravated the cyber risk climate (Slade, 2021). Evidence of this includes a mix of conceptual and empirical indicators for new threat vectors, new opportunities for attack, and an increase in the potential scope and impact of attacks (Wiggen, 2020). In this context, the notion of 'conceptual indicators' is used to describe factors likely to generate new opportunities for threat-actors (i.e. entities which seek to conduct cyber attacks), based on a first-principles approach. For instance, operational disruptions and shifts in the technological infrastructure such as those caused by remote working can increase the scope of cyber vulnerabilities for organisations and societies. Furthermore, a sudden change in the attack surface and working patterns of employees can nullify aspects of existing security policies or diminish their effectiveness. This is further exacerbated by the behavioural and psychological effects of the Pandemic on staff, as drivers of adherence to cybersecurity policies and best practices (Pfleeger and Caputo, 2012). The availability of key resource redundancy/buffers is also likely to be diminished, decreasing the ability of organisations to absorb incidents (Linkov and Kott, 2019).

In contrast, the notion of 'empirical indicators' is used to describe observed changes in the behaviour of threat actors, the opportunities and vulnerabilities that they exploit, and the impact of said exploitation. Following the National Institute of Standards and Technology (NIST), International Standards Organization, and European Network and Information Security Agency, Colorossi (2015, p. 507) summarizes the definition of the cyber vulnerability as "*…a flaw, weakness, or lack of security control in hardware, software, or a system process that exposes the system to compromise; simply stated, vulnerability is an exposure to compromise, and most system compromises are the direct result of exploitation of identified vulnerabilities*". In particular, during the COVID-19 lockdown, Jamilov *et al.* (2021) reported that the cyber vulnerabilities significantly increase in 2020 due to remote

work purposes with a large increase in the use of software. These spikes can also rise in the frequency of idiosyncratic and aggregate cyber incidents, which create an uncertain view of the future with regards to cyber security (Lallie *et al*., 2021). Thus, empirically, there is an accumulating body of evidence illustrating significant spikes in cyber threat activity and effects linked to the pandemic (Lallie *et al.,* 2021; Wirth, 2020; Newman, 2020; Wiggen, 2020; WHO, 2020), beyond its broader socio-economic impact (Nicola *et al.,* 2020).

The second operating assumption of this paper relates to the importance of better understanding the nature of the response by critical infrastructure to such an increase in cyberattacks and their potential scope and impact. This importance is anchored in two different lines of reasoning. Firstly, critical infrastructure organisations are, by definition, of essential strategic importance for nation-states and their economies (Alcaraz and Zeadally, 2015). Thus, understanding the response of such organisations to a crisis-based shift in the cyber risk climate is illustrative of the likely impact of potential incidents in key socio-economic settings. Secondly, given their importance, critical infrastructure organisations are the focus of extensive support and defensive efforts. This is exemplified by their scope in national security strategies, policy and regulatory considerations, as well as support frameworks. This is illustrated by the rebranding in 2018 of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity as the NIST Cyber Security Framework. Adjusting for other indicators (i.e. size, industry) should also indicate a relatively high level of capability and support availability, making such organisations exemplary instances of broader dynamics.
By acknowledging these two assumptions, we are faced with an empirical opportunity to complement the body of research tracking impacts following cyber breaches – a term used throughout the paper to denote incidents where the security of an organisation has been compromised (e.g. Kamiya *et al.,* 2018; Buckman *et al.,* 2018; Spanos and Angelis, 2016). We address this by exploring changes in investment and risk perception within critical infrastructure organisations in response to a general and discrete increase in their cyber risk climate. While not a substitute for incident impact studies, this approach mitigates some of the traditional issues affecting studies in the field. These include disincentives to disclose incidents (Amir *et al.,* 2018), incomplete impact data streams or asymmetries between precision and accuracy, a bias towards high-visibility, well-documented attacks, or an overrepresentation of specific organisational parameters — most notably, size (Rosati *et al.,* 2019, Hilary *et al.* 2016). Thus, by following the relationship between a model of

cybersecurity indicators/constructs and organisational response indicators in circumstances of crisis, we identify drivers of response patterns in investment amongst critical infrastructure organisations. More specifically, this approach is based on an exploration of the relationships between the perceived cybersecurity performance, perceived cyber risk and changes in cybersecurity investments as a result of a crisis. The value of the study is further enhanced by its focus on organisations from critical infrastructure sectors; the analysis of the perception of key cybersecurity performance indicators by senior managers and board members; and the COVID-19 pandemic as the context of the study.

2.2. Theoretical model and hypotheses development

To identify any relationships between cybersecurity performance indicators and crisis response patterns, a model of the two must first be outlined. The development of such a model involves a holistic perspective of the otherwise heterogeneous body of Organisational Cybersecurity literature, most notably frameworks and best practice. A comparative overview of key cybersecurity frameworks can be found in Azmi *et al.* (2018). Based on the research objective, such a model must achieve a series of key requirements. Firstly, it should include an ability to differentiate between core cyber capabilities and context- or maturity-dependent components, as a way to accommodate varied organisational profiles. In this context, both 'core capabilities and 'organisational profiles' are concepts adapted from the NIST Cybersecurity Framework (2018). We use the former to describe the essential infrastructure and abilities that organisations require in order achieve essential cybersecurity outcomes. The latter is used to denote the different needs, expectations and objectives that organisations can have, based on their domain of practice, technical complexity, strategy and other similar drivers of cyber risk tolerance. This is particularly important given the broad scope of the study, through its general focus on critical infrastructure organisations.

Secondly, a distinction between cybersecurity and resilience should be made which reflects key differences in orientation between the two constructs (WEF, 2017). Bjorck *et al.* (2015:313) highlight how, in contrast to cybersecurity, a cyber resilience-based approach "must take the business as a starting point, rather than information technology". This indicates a more holistic focus when considering potential incidents, exploring their potential effects on the organisation and on its ability to sustain business delivery in the context of failures. Furthermore, the authors also flag a shift in perspective between the two approaches: cybersecurity primarily aims to avoid incidents/failures, whereas cyber resilience primarily

aims to ensure survival and adequate performance despite potential incidents/failures. When, looked at from a cyber resilience perspective, incidents should be explored in the physical, informational, cognitive and social domains – forming a broad, holistic perspective, rather than a (solely) technical one (Linkov and Kott, 2019). Despite the clear overlap between the two approaches, they differ in their baseline assumption regarding the possibility of avoiding cyber incidents. This is summarised by Bjorck *et al.* (2015:313) as a difference in intention: 'fail-safe' for cybersecurity, and 'Safe-to-fail' for cyber resilience.

Finally, the model should consider preparedness and adaptive mechanisms such as situational awareness and learning at individual, team and organisational levels. Integrating and learning from the different functions involved (e.g. information security management, incident response) would help organisations not only respond to security incidents when faced with a crisis, but also proactively manoeuvre the threat environment (Ahmad et *al*., 2020). Each of these conditions is addressed and further elaborated in the following subsections.

The first construct introduced by the model is '**Focus' [Core]**. The 'Focus' construct aims to encompass general, foundational elements of a cybersecurity framework. These include explicit consideration for (1) the effectiveness of basic controls such as detection, mitigation and response; (2) the inclusion of cybersecurity within the organisation's policy; and (3) the existence and regular review of a crisis/incident response plan. Collectively, these dimensions can be seen as a shared core among organisations seeking an active stance concerning cyber threats, regardless of their scale, their threat climate, or level of sophistication of their defensive apparatus. At a basic level, the 'Focus' construct attempts to capture a sense of intentionality within the organisational management structures concerning cybersecurity. Additionally, we use 'Focus' to refer to the *ability* of the organisation to detect, mitigate and respond to cybersecurity incidents. By *ability* we refer to the presence of the relevant cybersecurity infrastructure, systems and provisions within the organisation. As a result of this, 'Focus' reflects elements that are common across cybersecurity frameworks –i.e. frameworks and systems for information security management, with varying degrees of specificity and prescription. Notable examples include the UK's cyber essentials scheme, the ISO 27000 family of standards, and the NIST cybersecurity framework (ISO/IEC, 2018; NIST, 2018). While varied in their orientation and level of abstraction, the presence of these frameworks illustrates the importance of such a foundation, while also outlining a functional structure for the implementation of information security management strategies. In summary,

the ‘Focus’ construct encompasses a common denominator of key pre-requisites for more complex cyber security management initiatives.

The second construct we introduce is **‘Capability’ [More]**. ‘Capability’ captures higher-order specifications, characteristics, and good practices associated with cybersecurity performance. Notably, it reflects cybersecurity capabilities which can vary based on functional maturity levels (Miron and Muita, 2014) and security environments. These include (1) a sufficient technological understanding at a board level for effective governance (Rothrock *et al.,* 2018; Nolan *et al.,* 2019); (2) the existence and adequacy of an infrastructure for managing cyber intelligence (NIST, 2018); (3) an understanding of the interdependence between digital assets and services in an enterprise performance context; (4) mechanisms for communicating relevant incidents; and (5) involvement in domain-specific information and knowledge sharing partnerships. Unlike ‘Focus’, the ‘Capability’ construct goes beyond capturing basic intentionality, awareness and controls. Instead, ‘Capability’ seeks to capture variety in organisational capability and requirements –a concept introduced in the NIST Cybersecurity Framework (CSF) through the inclusion of ‘implementation tiers’ (NIST, 2018). While loosely modelled around components of the CSF’s tier structure, the ‘Capability’ construct does not seek to develop a hierarchy of organisational requirements or maturity levels. Instead, it seeks to enable the identification of relationships between the covered indicators and the organisational approach to crisis response. This is subsequently reflected in the associated questions designed to operationalise the construct (Appendix A).

The third component of the model is **‘Resilience’ [Resilience Profile]**. A diverse, growing body of literature highlights the importance of organisational cyber resilience (WEF, 2017; NCSC NZ, 2019; BSI 31111:2018). In this context, cyber resilience is distinguished from cybersecurity by describing an organisation’s ability to absorb and overcome successful cyberattacks while maintaining core function (Bjorck *et al.,* 2015; Rothrock *et al.,* 2018). While models of cyber resilience do exist in both academic and grey literature, they vary across levels of analysis, methods of development and objectives –i.e. descriptive vs. prescriptive models. Nonetheless, most models share a focus on an organisation’s ability to maintain function and identity following cyber incidents, which complements other anticipatory and mitigative measures. As such, the emerging model employs a simplified, high-level view of cyber resilience based on three core dimensions of such an ability: their regulatory, functional, and digital redundancy/vulnerability dimensions. This includes

ensuring legislative compliance, a sufficient functional budget for necessary cyber response, and an ability to ensure business continuity if access to digital assets is disrupted. In other words, 'Resilience' is constructed based on regulatory compliance, defensive capital, and digital asset (in)dependence/redundancy. The absence of any of these components is likely to significantly affect an organisation's ability to sustain its operations following a cyberattack.

Finally, the '**Prep' [Integration]** construct focuses on the intellectual capital development within the firm. 'Prep' engages themes surrounding training and preparation both for executives and operational employees. 'Prep' emerges from our understanding of intellectual capital as a core pillar for meta-disciplinary inquiry into a strategic perspective of cybersecurity. Cybersecurity is a fast-evolving domain and, as such, the capabilities required to effectively manage this challenge within the organisation are highly dynamic. For the majority of employees and management boards such special skills and knowledge fall within what Acemoglu and Pischke (1999) described as the category of capabilities that cannot be provided in the course of general education and therefore require an investment in the workforce. Given the role that intellectual capital play in supporting an organisation's situational awareness and adaptive capacity when faced with structural disruptions and changes in risk, training and preparation both for executives and operational employees have been delineated as a distinct component of the model. This enables exploring potential relationships between the levels of preparedness of decision-makers and organisational response to a crisis. Particularly, a focus on the approach to training and development and the infrastructure supporting such processes enables accounting for the cognitive challenges affecting cyber situational awareness through disruptive change. Subsequently, the 'Prep' construct maps the presence of a regular review process of the role and degree of the integration of cybersecurity in operations, the extent to which cybersecurity is a priority for the management board, the existence of board-level cyber skills development initiatives (i.e. war games), and the perceived efficacy of employee cybersecurity training programmes (Weill *et al.,* 2019).

2.3. Modelling Response

Modelling response patterns following a shift in the risk climate can also involve tremendous variability, especially when the group under observation is defined primarily by the societal function and domain, rather than economic or organisational parameters. Effective cybersecurity in critical infrastructure organisations can vary greatly based on their size, area

of operation, technological dependence and business model, assets, context and interdependence to other high-risk stakeholders. This, in turn, affects the scope and nature of what can be considered meaningful responses to a change in the risk climate. Furthermore, the unprecedented nature of the COVID-19 crisis has created novel territory for the largely prescriptive frameworks (Moore *et al.,* 2015) which dominate an otherwise arguably problematic knowledge domain (Sallos *et al*., 2019). It should also be recognised that different types of critical infrastructure organisations are likely to be affected in different ways in a broader enterprise risk context, which can affect the perception, response and prioritisation of cyber risk shifts.

In response to this variability, the model will use two common denominator constructs which are not inherently sensitive to the previously identified potential idiosyncrasies, namely *senior managers' risk perception* and *investment patterns*. More specifically, given the recent unprecedented change in the risk climate, we seek to identify the drivers of an organisational (i.e. senior management) change in Cybersecurity Risk Perception [Risk], and Cybersecurity Investment patterns [Investment]. The former reflects an indicator of shared situational awareness, while the latter relates to changes in resource allocations following the crisis –a key proxy indicator of executive and relative prioritisation and action (Moore *et al.,* 2015, Benaroch, 2002). While simplistic, this response component enables tracking the effects of various cybersecurity indicators (e.g. compliance to policy, functional budget sufficiency, effective communication mechanisms and partnerships, etc.), as codified through the first four constructs of the model, across different organisations through a logic of perception and response. By distinguishing between these two elements, Risk and Investment enable a richer interpretation of findings, as more scenarios and patterns can be inferred.

2.4. Hypotheses

Having defined *Focus*, *Capability*, *Resilience* and *Prep* as key cybersecurity performance indicators contributing to a holistic perspective of organisational cybersecurity, we sought to explore the relationships between those constructs and with what is considered effective cybersecurity frameworks and good practice. Our analysis remained focused on differentiating between core cyber capabilities and cybersecurity maturity, considering the preparedness and adaptive mechanisms that can affect the way organisations respond to a crisis. With this in mind the following hypotheses were defined:

Hypothesis 1. The Focus–Investment interdependencies:

In an attempt to understand the interrelations between an organisation's focus on its cybersecurity foundations and a shift in its cybersecurity investments following a crisis, we hypothesise that:

> *A critical infrastructure organisation's provision of foundational cybersecurity elements [Focus] is positively correlated to a shift in cybersecurity investments [Invest] following a change in the risk climate.*

Hypothesis 2. The Capability–Investment interdependencies:

With an aim to investigate the extent to which the presence of higher-order cybersecurity capabilities/best practices is positively correlated to a shift in cybersecurity investments following a crisis, we hypothesise that:

> *Indicators of higher-order cybersecurity capabilities/best practices in critical infrastructure organisations [Capability] are correlated to a shift in cybersecurity investments [Investment] following a change in the risk climate.*

Hypothesis 3. The Resilience–Investment interdependencies:

Our efforts to understand the association between organisational cyber resilience and adaptive changes in its cybersecurity investments following a crisis let to the formulation of the following hypothesis:

> *Indicators of cyber resilience in critical infrastructure organisations [Resilience] are associated with a shift in cybersecurity investments [Investment] following a change in the risk climate.*

Hypothesis 4. The Intellectual Capital–Investment interdependencies:

As we sought to understand the correlations between an organisation's cybersecurity training and preparation efforts and the changes in its cybersecurity investment following a crisis, the following hypothesis was proposed:

> *A critical infrastructure organisation's cybersecurity training and preparation efforts for its operational staff and executives [Prep] are associated with a shift in cybersecurity investments [Investment] following a change in the risk climate.*

Hypothesis 5. The Risk–Investment interdependencies:

Finally, we sought to understand how C-level executives change their attitude towards cybersecurity based on their perception of changes in their cyber risks environment, through the study of the following hypothesis:

> *Senior managers' and executives' perception of an increase in the cyber risk climate [Risk] is associated with changes in their cybersecurity investments [Investment] in the context of a crisis.*

The combination of these five hypotheses leads to the theoretical framework in figure 1.

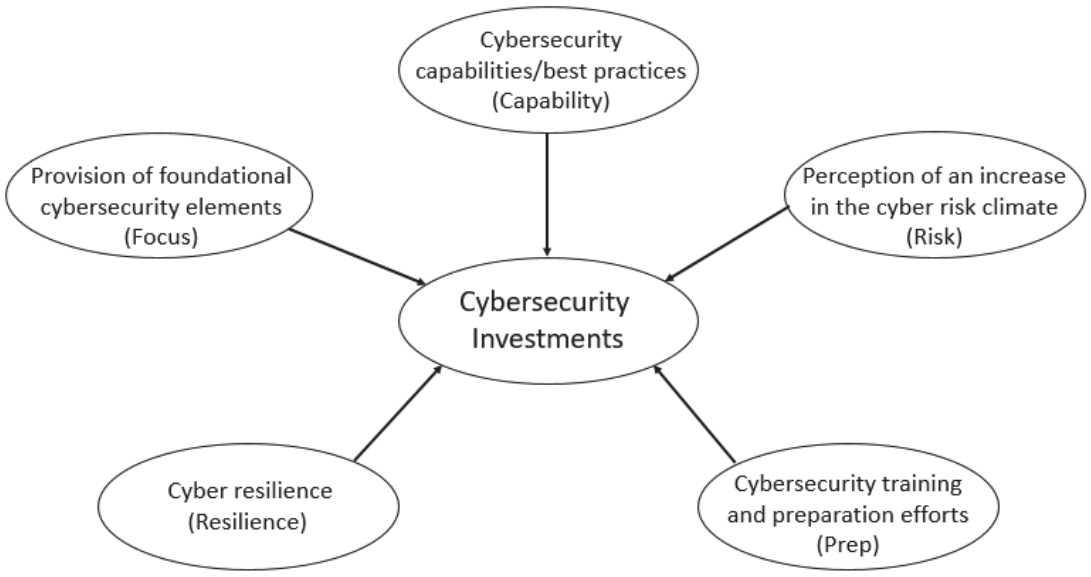

Figure 1. Theoretical Framework

3. Data and Methodology

3.1. Data and Descriptive Statistics

This study focuses on analysing indicators affecting organisational response to a cyber crisis (COVID-19) pandemic. To that aim, primary data was collected from 400 C-level executives including directors, owners and other individuals holding senior positions in organisations from critical infrastructure sectors in the UK at the peak of the COVID-19 pandemic, in July 2020. Approximately 21.8% are the organisation owners, followed by president, chairman, CEO and general manager (20.0%), Chief Information Officer (CIO) (15.0%) and Chief Financial Officer (CFO) (12.0%). The research focused on organisations from the manufacturing, energy, transport, finance, healthcare, agriculture and communications sectors. The sectors with higher representation in the sample were healthcare (24.8% of the sample), finance (23.0%) and manufacturing industries (21.0%). Approximately 62.5% of the

total sample consisted of Small- and Medium-sized Enterprises (SMEs), while 37.5% were large enterprises.

An online questionnaire was designed using 5-Likert Scale for all questions, ranging from 1 (Strongly disagree) to 5 (Strongly agree), to capture the individuals' perception of *Focus*, *Capability*, *Resilience* and *Prep* as key cybersecurity performance indicators potentially contributing to a holistic perspective of their organisations' cybersecurity. A telephone survey was administered in July-August 2020, around 3 months after the World Health Organisation (WHO) had declared the COVID-19 outbreak as a pandemic on the 11 March of that year. By that time, most UK organisations had been impacted by the socio-economic crisis that was derived from the pandemic.

Table 1 details the descriptive statistics and description of variables used in the analysis. For example, for the [Capability] construct, the information related to having a sufficient understanding of organisation's key digital assets and services (ASST) is rated as the highest average level of 3.92, followed by having effective mechanisms in place for the production, analysis and utilisation of cyber intelligence (MECH) (3.89) and having efficient mechanisms in place for external communication with the potentially affected parties (COMM) (3.88). The majority of the directors in these sectors tend to report "agree" for these questions since the median reports the value of 4. For the [Focus] construct, the organisations' information on security policy relating to cybersecurity (POLY) has the highest average level of 4.10. The average level of the up-to-date information security policy on cybersecurity legislation (LEGS) has the highest level for the [Resilience] construct, with the value of 4.04. Additionally, the effective training and awareness programme on cybersecurity (TAIN) and an increase in the cybersecurity risk related to the COVID crisis for the organisation (CYBS) are rated as the highest average level for the [Prep] and [Risk] construct, respectively.

Table 1 Summary of statistics for indicator variables

Indicator	Description	Obs.	Mean	SD	Median
Capability DIGT	Our management board has a sufficient understanding of the threats digital technologies currently pose to our organisation	393	3.858	1.127	4

MECH	Our organisation has effective mechanisms in place for the production, analysis and utilisation of cyber intelligence (i.e. identification of risks and threats)	396	3.894	1.093	4
ASST	Our organisation has a sufficient understanding of our key digital assets and services, and the interdependencies between them	396	3.924	1.060	4
COMM	In the event of a cyber security incident, our organisation has efficient mechanisms in place for external communication with the potentially affected parties	397	3.882	1.070	4
PART	Our organisation is involved in a programme or external partnership for the sharing of cyber security information, expertise, technology and/or resources, as and when required	384	3.677	1.192	4
Focus DECT	Our organisation has effective measures in place for the detection, mitigation and response to cyber security incidents	393	3.863	1.070	4
POLY	Our organisation's information security policy includes measures related to cyber security	261	4.100	0.960	4
REVW	Our organisation regularly reviews our cyber crisis or incident response plan	233	4.060	0.879	4
Resilience LEGS	Our organisation's information security policy is updated as required to comply with cyber security legislation	263	4.042	0.997	4
BUDG	The budget our organisation has allocated to cyber security is sufficient	220	3.936	0.944	4
CRIT	Our organisation has effective measures in place to remain operational even if we lose access to a critical digital asset (e.g. a particular database or application)	397	3.909	1.045	4
Prep TOPP	Cyber security is one of the top priorities for our management board	387	3.726	1.182	4
MEAS	Our organisation regularly measures the extent to which cyber security is embedded in our operations	394	3.678	1.196	4
TAIN	Our organisation's training and awareness programme on cyber security for employees is effective	249	4.024	0.946	4

TABT	Our management board regularly participate in cyber security exercises such as table-top and cyber wargames	392	3.617	1.252	4
Risk DATB	The risk of a data breach for our organisation has increased during the current COVID-19 crisis	397	3.549	1.225	4
CYBS	The current COVID-19 crisis has increased the cyber security risk for our organisation	396	3.611	1.206	4
Cyber investment (INVEST)	Our organisation's investment in cyber security has changed as a result of the current COVID-19 crisis	394	3.579	1.209	4

3.2 Data Analysis: Partial Least Square Structural Equation Modelling (PLS-SEM)

We used Partial Least Square Structural Equation Modelling (PLS-SEM) to understand the perception of individuals holding senior positions in organisations from critical infrastructure sectors in the UK about their organisations' cybersecurity. PLS-SEM allowed us to analyse the relationships between their perceived cybersecurity performance, perceived cyber risk and changes in cybersecurity investments as a result of the COVID-19 crisis. PLS-SEM performs like a multiple regression analysis (Hair *et al*., 2014), allowing for exploring possible causal relationships and more complex relationships (Hair *et al*., 2006; Hair *et al*., 2017). It is widely used to deal with data-related threats such as small sample size, non-normal data, and formatively measured constructs (Hair *et al*., 2014; Henseler *et al*., 2017; Ridon *et al*., 2017: Cepeda-Carrion et al., 2019). PLS-SEM is also appropriate for theory building and hypothesis testing (Haddoud *et al*., 2016), and it has less rigorous requirements for restrictive assumptions, which is a useful tool to develop and estimate such models by enabling them to avoid additional limiting constraints (Hair *et al*., 2017). To test the hypotheses, in our case all measures used in the structural model framework (Figure 2) were considered as composites Mode A, which are refractive constructs (Cepeda-Carrion *et al*., 2019). Therefore, PLS-SEM is the most suitable technique for data analysis for this model (Richter and Cepeda, 2016), in which the total variance of all constructs is used to estimate model parameters (Hair *et al*., 2017).

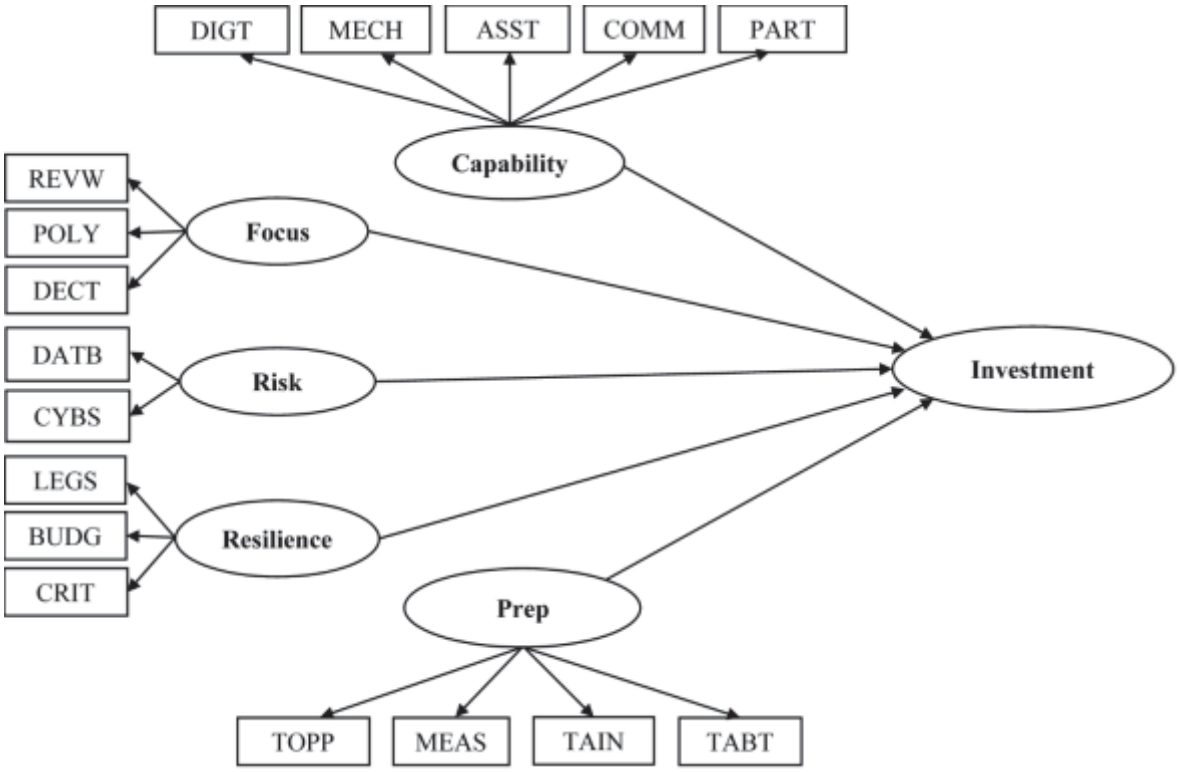

Figure 2 Structural Model Framework

For the data analysis, this study uses the SmartPLS 3 to run PLS-SEM. Following the recent requirements for reporting the results of PLS-SEM (Henseler *et al*., 2016; Hair *et al*., 2019) and the call for the emancipation of PLS-SEM because of the different epistemological nature of the measures (common factor versus composites) (Rigdon, 2016; Rigdon *et al*., 2017), we firstly consider the goodness of fit for the model using the standardised root means square residual (SRMR). For our model, the value of SRMR is 0.079, which is less than 0.1 (Henseler *et al*., 2014; Mehmet and Jakobsen, 2017) and is also below 0.08 which is a more conservative version proposed by Hu and Bentler (1998). Also, we apply the Unweighted Least Squares (d_ULS) and Geodesic discrepancies (d_G) to consider the exact model fit which are below the 99%-quantile of the bootstrap discrepancies (Dijkstra and Henseler, 2015). Consequently, our model satisfied the level of goodness of fit (Henseler *et al*., 2014; Hair *et al*., 2017).

When the model has passed the satisfactory level of the model fit, the assessment of the measurement model is required to verify the measurement reliability and validity. The confirmatory composite analysis is a recent global measure of it. To do this, we checked the internal consistency reliability by assessing the Dijkstra-Henseler's rho (ρA), composite

reliability (CR), and Cronbach's alpha (CA). If f the values of the internal consistency reliability are between 0.70 (minimum) and 0.90 (maximum threshold), the variables used in the model are reliable (Hair *et al*., 2019). We also assessed the convergent validity by considering the values of average variance extracted (AVE). If the AVE values of all the constructs are greater 0.5 at the construct level, the measurement model's convergent validity is acceptable (Henseler *et al*., 2016; Hair *et al*., 2017). Table 1 reports the values of ρ_A, CR, CA, and AVE. All values are above the common threshold values (Henseler *et al*., 2015; Henseler *et al*., 2016; Hair *et al*., 2019), indicating that all variables in the model are reliable. Moreover, following Henseler *et al*. (2014) we checked the discriminant validity by analysing heterotrait-monotrait ratios of correlations (HTMT). If the value of HTMT is lower than the threshold value of 0.90, evidence for the discriminant validity is therefore provided (Henseler *et al*., 2014; Hair *et al*., 2019). Table 3 reveals all values of HTMT for our model which are below the recommended threshold. Therefore, we can confirm that our constructs (latent variables) are reliable to test the causal relationship of the proposed structural model (Figure 2).

Table 2 Assessment of Measurement Items, Construct Reliability and Validity

Construct	**Variable**	**Loading**	**Cronbach's Alpha**	**Rho_A (ρ_A)**	**CR**	**AVE**
Capability			**0.766**	**0.807**	**0.862**	**0.635**
	DIGT	0.632				
	MECH	0.785				
	ASST	0.777				
	COMM	0.749				
	PART	0.779				
Focus			**0.767**	**0.726**	**0.769**	**0.518**
	DECT	0.838				
	POLY	0.671				
	REVW	0.791				
Resilience			**0.760**	**0.765**	**0.779**	**0.529**
	LEGS	0.779				
	BUDG	0.663				
	CRIT	0.713				
Prep			**0.709**	**0.752**	**0.817**	**0.598**
	TOPP	0.779				
	MEAS	0.816				
	TAIN	0.651				
	TABT	0.780				
Risk			**0.724**	**0.729**	**0.878**	**0.815**
	DATB	0.872				

	CYBS	0.898				

Notes: Rho_A (ρA) = Dijkstra-Henseler's rho; CR = Composite Reliability; AVE is Average variance extracted.

Table 3 the Discriminant Validity Values - Heterotrait-Monotrait Ratio (HTMT)

	(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**
Capability (1)						
Focus (2)	0.823					
Resilience (3)	0.793	0.711				
Prep (4)	0.749	0.809	0.639			
Risk (5)	0.673	0.566	0.523	0.821		
Investment (6)	0.530	0.505	0.457	0.633	0.674	

4. Results of the Structural Model using PLS_SEM

After verifying the reliability and validity of the measurement model, Table 4 and Figure 3 report the results of the structural model of the association between the indicators of board's perception of the cybersecurity of their organisation and the cybersecurity investment patterns during the COVID-19 pandemic (Figure 2), which include the path coefficients (β) and the p-values of the relationships hypothesised in this study. The value of R^2 is 0.407, indicating that 40.7% of the total variance is explained by the endogenous latent variables in the structural model, which is substantial (Hair *et al.*, 2019; Addae *et al.,* 2019). We also use a bootstrapping sampling (5,000 samples) to determine the significance of the path coefficients[1]. The key findings show that the effective integration of cybersecurity governance on the management board's strategy [Prep] is positively and significantly associated with the organisation having prioritised investment in cybersecurity during the COVID crisis [Investment], which is consistent with H4. Also, we found that the management board's perception of cyber risk [Risk] is positively and significantly associated with the organisation having prioritised investment in cybersecurity [Investment], which support H5.

[1] Although the total sample is 400 observations, the information used in the analysis is only available for 114 observations. Therefore, we use the PLS-SEM with bootstrapping with 5,000 samples to evaluate the significance of path coefficients (Streukens and Leroi-Werelds 2016).

Table 4. The results of the structural model and hypothesis testing

Hypothesis	Structural Path	Path Coefficient (β)	P-Value	Decision
H1	Capability→Investment	0.108	0.376	Do not support
H2	Focus→Investment	0.091	0.127	Do not support
H3	Resilience→Investment	-0.020	0.719	Do not support
H4	Prep→Investment	0.245**	0.001	Support
H5	Risk→Investment	0.463**	0.000	Support

Note: ** is the significance level of 0.05.

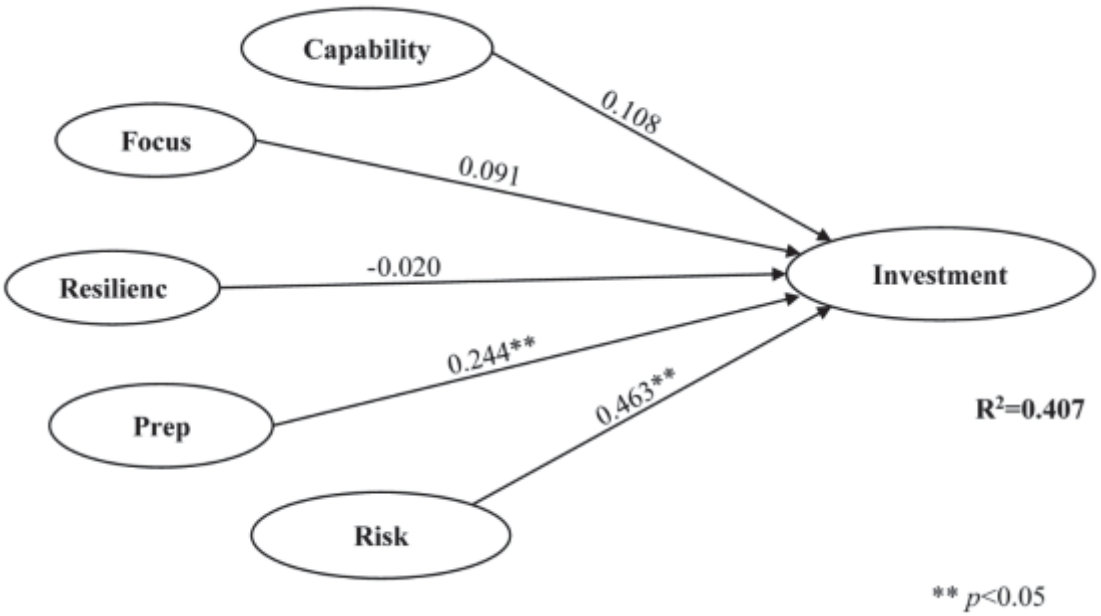

Figure 3. Results of PLS-SEM

5. Discussion

Our research has found a significant positive correlation between an organisation's (i.e. senior management) perception of a change in its cybersecurity risk [Risk] and its patterns of investment in its own cybersecurity [Investment] in critical infrastructure organisations. This finding supports our hypothesis 5. While intuitive, this relationship is meaningful as it suggests a direct link between senior managers' perception of an increase in the cyber risk and their efforts to respond to such a shift through investments in cybersecurity. With this, we

add a practical perspective to theoretical views of a crisis as a key proxy indicator of executive and relative prioritisation and action, by highlighting the correlation – in practice, between shared cyber situational awareness and changes in cyber resource allocations derived from the COVID-19 pandemic. Beyond the proposed 'perception (of risk) - action (cyber investment)' relationship between the two constructs, this result also suggests that changes in investment patterns following a shift in risk are a potentially meaningful indicator of response. In other words, if senior managers perceive a potential increase in cyber risks, a shift towards investment is likely to follow (Department for Digital, Culture, Media and Sport 2021). And, respectively, the relationship highlights how potential responses to an increasingly hostile risk climate are conditioned by managers' perception/situational awareness. While not fully explored within the context of the paper, the factors which correlate with such an increase in risk perception merit further investigation. Finally, this line of analysis enables scholars and practitioners to avoid in their practices the idiosyncrasies of specific incidents by focusing on anticipatory/capability-related mechanisms rather than incidents/response. In other words, this finding supports Sallos's *et al*. (2019) views of cybersecurity as a knowledge problem, pointing to cybersecurity as a critical capability within organisations, closely dependent on the intellectual capital base and particularly relevant in critical infrastructure sectors.

We have also found a positive correlation between the efforts placed by critical infrastructure organisations in the development of their intellectual capital in the cybersecurity domain (i.e. cybersecurity training and preparation) [Prep] and the changes in investment in their cybersecurity [Investment] following a crisis. This finding supports our hypothesis 4. A plausible interpretation of this is that organisations which prioritise cybersecurity as a board-level concern are more likely to have changed their cybersecurity investments following the COVID-19 crisis. In fact, those organisations that regularly bring cybersecurity to their boardroom, where it is likely to be addressed from perspectives such as Human Resource development, would regularly review the scope and relevance of cybersecurity within their operations, and therefore are more likely to possess an active –and potentially more effective, training infrastructure for both employees and managers (Rothrock *et al*., 2018). Again, this phenomenon can be explained through Sallos's *et al*. (2019) knowledge-based view of cybersecurity: such organisations have functional mechanisms for feedback acquisition and dissemination which support adaptation to a change in their environment. Respectively, they are more likely to perceive and contextualise a shift in the cyber risk climate in their shared,

possibly organisation-specific models of cybersecurity and act accordingly. The finding is also aligned with the views of scholars such as Al-Awadi and Renaud (2007), Disparte and Furlow (2017) and He *et al*. (2019), who have highlighted over the last two decades the need for organisations to invest in regular cybersecurity awareness training for all personnel to prevent more data breaches to their intellectual capital.

It should be reemphasised that in this context, however, that 'a change' in investment is not necessarily related to 'an increase' in investment. Rather, our result indicates that such organisations are more responsive to operational changes which likely shift the relative scope of cyber risk in an enterprise risk context. It should also be highlighted that, given the associated expenditure and cyber maturity, the organisation's efforts on cybersecurity training and preparation of their operational staff and executives [Prep] are also likely to correlate with organisational size and domain of operation.

Our research did not find a significant correlation between the presence of higher-order cybersecurity capabilities/best practices [Capability] in organisations from critical infrastructure sectors and a shift in their cybersecurity investments [Investment] following a change in the risk climate, as initially hypothesised (H1). Similarly, the data did not support a direct correlation between a critical infrastructure organisation's cyber resilience [Resilience] and their adaptive changes in cybersecurity investments [Investment] following a crisis (H3). This lack of a direct relationship between the proposed indicators is in itself a potentially significant finding. Beyond methodological effects –further explained in the Limitations section, both hypotheses present weak negative relationships between the modelled key cybersecurity performance indicators. The absence of a correlation between Resilience and shifts in Investment is seemingly counterintuitive. This is due to a consistent theoretical association between resilience and adaptation/adaptive capacity. However, at an operational level, the Resilience construct primarily covers a perceived sufficiency of cybersecurity performance, expressed through compliance, functional budget sufficiency, and ability to absorb incidents/disruptions relative to critical digital assets. Organisations scoring highly on these measures would plausibly express –or at least perceive, lower relative levels of vulnerability to cyber incidents. Furthermore, the inclusion of 'budget sufficiency' as a component of resilience is likely to affect the relative effectiveness of investment as an indicator of response. At a broader level, organisations may score highly in resilience due to a variety of reasons which could also affect investment patterns. These can include resource

availability, operational domain and model –which are particularly noteworthy when it comes to the scope of digital assets in the context of value creation, organisational size, and levels of situational awareness, none of which are accounted for by the construct. The same line of argumentation holds true for Focus (H2) as a construct, which covers general elements and mechanisms which underpin cybersecurity infrastructure.

5.1. Theoretical significance and practical contributions

This research makes a significant contribution to the academic literature by highlighting the importance of intellectual capital development as a basis of a successful cybersecurity management strategy. A knowledge-based view of cybersecurity enables the required levels of cyber situational awareness in the board through investments in both intellectual capital and cybersecurity management development. Thus, our findings open new avenues for research and practice in management sciences, particularly in the domains of intellectual capital management, digital resilience, disaster management and business continuity.

The results show that effective adoption of the latest technologies and their applications relies on the understanding at all levels within the organisation of the risks involved. We have put our emphasis on the role of the management board particularly in organisations from critical infrastructure sectors in the dynamic socio-economic context where these operate and given the wide-range implications of their resilience. The work also builds on the emerging body of work calling for the exploration of cybersecurity as an important Intellectual Capital concern (Renaud *et al.*, 2019; Sallos *et al.*, 2019; Balozian *et al.,* 2021).

In addition, this work contributes to the conceptual understanding of important facets of the concept of digital resilience, which is key to the current and future efforts towards the digital transformation of business and society. By identifying a series of indicators of performance, governance and management of cyber risk, as perceived by senior management in critical infrastructure sectors, our research informs future theoretical developments and management practice. For example, as scholars and practitioners refer to both cybersecurity and intellectual capital as true capital costs despite the perceived differences between the two domains, we foresee that future studies will study the relationship between the cost associated to intellectual capital developments and that of recovering from a cybersecurity incident.
An additional contribution of this paper is derived from the study of management perception of the subject when they have been faced with external pressures, disruptions, or abnormal

circumstances in the form of a pandemic. At the time of writing, the relationships between senior management's perception of cybersecurity risks and performance, and the changes they make in cybersecurity investments as a result of a crisis had not been studied. Our focus on those issues in organisations from critical infrastructure sectors during the COVID-19 pandemic also make ours a unique contribution to both research and practice.

6. Conclusion

This research has studied the relationships between the board's perception of their cybersecurity performance, the dynamic cyber risk climate and changes in cybersecurity investments in the context of critical infrastructure organisations as a result of a crisis. We found a significant positive correlation between an organisation's perception of a change in its cybersecurity risk and its patterns of investment in its own cybersecurity in critical infrastructure organisations. Similarly, we found that a positive correlation exists between the efforts placed by critical infrastructure organisations in cybersecurity training and the changes in investment in their cybersecurity, particularly in relation to their intellectual capital development efforts, i.e. building the knowledge base of their operational staff and executives. Thus, this finding contributes to emerging lines of enquiry within Intellectual Capital and Cybersecurity Management research initiated by Renaud *et al.,* (2019) and Sallos *et al.*, (2019). Paradoxically, we found that a change in senior managers' strategy for cybersecurity investments following the COVID-19 pandemic was neither correlated to their perception of cyber resilience nor to the presence of higher-order cybersecurity capabilities/best practices. As discussed in previous sections, this lack of a direct relationship between the proposed indicators became in itself a potentially significant finding. We have therefore defined and addressed issues of significant importance for businesses and societies, and raised awareness of the need for further research to understand the socio-economic impact cybersecurity management.

6.1. Limitations and avenues for future research

Despite its valuable insights, the research has limitations which offer avenues for further research. First, the heterogeneity of the population –senior managers from critical infrastructure organisations, does not allow for granularity in meaningful factors such as the size, domain of operation or technological maturity of the organisations studied. In particular, our research focused on organisations of any size.

Another key factor that may have influenced the research is the fact that not all interviewees may have been fully capable of making an accurate assessment of the cyber security and digital resilience of their organisations, despite their role as C-level executives –be it directors, owners or individuals holding senior positions. This is due to both the complexities of the problem and the limited knowledge of cyber risks and vulnerabilities currently available to organisations in a format that can inform management decisions. In this direction, the authors acknowledge that this research has had an essentially exploratory nature and therefore it is recommended that these issues be explored in subsequent research.

It should also be highlighted that, given the associated expenditure and cyber maturity, the organisation's efforts on cybersecurity training and preparation of their operational staff and executives are also likely to correlate with organisational size and domain of operation. In terms of our model, it is important to recognise that while its constructs map to well-researched themes, these represent the complex socio-technical phenomena and therefore their scope has been reduced to manageable concepts for the purpose of this research. The complexities associated to the concept of digital risk is an example of this. While not fully explored within the context of the paper, digital risk perception and the factors which correlate with it merit further investigation.

Further research to address the above areas is encouraged, with a view to continue to expand on the theoretical and practical benefits of moving from an overly technical approach to cybersecurity to a broader understanding of digital resilience as a knowledge problem for business and society.

References

Acemoglu, D. and Pischke, J. S. (1999). Beyond Becker: Training in imperfect labour markets. *The economic journal*, Vol. 109 No. 453, pp. 112-142.

Addae, J.H., Sun, X., Towey, D. and Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. *User Modeling and User-Adapted Interaction*, Vol. 29 No. 3, pp. 701-750.

Ahmad, A., Desouza, K.C., Maynard, S.B., Naseer, H., and Baskerville, R.L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, Vol. 71 No. 8, pp. 939-953.

Al-Awadi, M. and Renaud, K. (2007). 'Success factors in information security implementation in organizations', in Kommers, P. (Ed), International Association for the Development of the Information Society (IADIS) International Conference on e-Society, pp. 169-176.

Alcaraz, C. and Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, Vol. 8 No. C, pp. 53–66.

Amir, E., Levi, S. and Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, Vol. 23 No. 3, pp. 1177–1206.

Azmi, R., Tibben, W. and Than Win, K. (2018). Review of cybersecurity frameworks: context and shared concpets. *Journal of Cyber Policy,* Vol. 3 No. 2, pp. 258-283.

Balozian, P., Leidner, D. and Xue, B. (2021). Toward an intellectual capital cyber security theory: insights from Lebanon, *Journal of Intellectual Capital*. Emerald Publishing Limited, (ahead-of-print), https://doi.org/10.1108/JIC-05-2021-0123

Benaroch M. (2002). Managing Information Technology Investment Risk: A Real Option Perspective. *Journal of Management Information Systems*, Vol. 19 No. 2, pp. 43-84.

Björck, F., Henkel, M., Stirna, J. and Zdravkovic, J. (2015). Cyber resilience – Fundamentals for a definition. *Advances in Intelligent Systems and Computing*, Vol. 353 No. 7, pp. 311–316.

Buckman, J., Hashim, M. J., Woutersen, T. and Bockstedt, J. (2018). *Fool Me Twice: Data Breach Reductions Through Stricter Sanctions*. SSRN, https://doi.org/10.2139/ssrn.3258599

Cepeda-Carrion, G., Cegarra-Navarro, J.-G. and Cillo, V. (2019). Tips to use partial least squares structural equation modelling (PLS-SEM) in knowledge management. *Journal of Knowledge Management*. Vol. 23 No. 1, pp. 67-89.

Colorossi, J.L. (2015), 'Cyber security', Davies, S.J., Hertig, C.A. and Gilbride, B.P. (Eds), *Security Supervision and Management,* (4th Ed), Butterworth-Heinemann, Oxford, UK, pp. 501-525.

Dabić, M. Vlačić, B., Scuotto, V. and Warkentin, M. (2021). 'Two decades of the Journal of Intellectual Capital: a bibliometric overview and an agenda for future research', *Journal of Intellectual Capital*, Vol. 22 No. 3, pp. 458-477. https://doi.org/10.1108/JIC-02-2020-0052

Dijkstra, T.K. and Henseler, J. (2015). Consistent and Asymptotically Normal PLS Estimators for Linear Structural Equations, *Computational Statistics & Data Analysis*, Vol. 81 No. 1, pp. 10-23.

Disparte, D. and Furlow, C. (2017), "The best cybersecurity investment you can make is better training", *Harvard Business Review*, pp. 2-4, available at: https://hbr.org/2017/05/the-best-cybersecurity-investment-you-can-make-is-better-training (accessed 30 September 2021)

Fornell, C. and Larcker, D.F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, Vol. 18 No. 1, pp. 39-50.

Geneva, World Economic Forum (WEF). (2017). 'Advancing Cyber Resilience: Principles and Tools for Boards', available at: http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf (accessed 27 September 2021)

Geneva, World Economic Forum (WEF). (2019). 'The Global Risks Report 2019', available at: https://www.weforum.org/reports/the-global-risks-report-2019 (accessed 27 September 2021)

Geneva. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). (2018). 'Information technology - Security Techniques - Information security management systems - Overview and vocabulary. ISO/IEC 27000', available at: https://www.iso.org/isoiec-27001-information-security.html (accessed 27 September 2021)

Geneva. World Health Organization (WEF). (2020). 'WHO reports fivefold increase in cyber attacks, urges vigilance', available at: https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance (accessed 27 September 2021)

Haddoud, M.Y., Jones, P. and Newbery, R. (2017). Export promotion programmes and SMEs' performance: Exploring the network promotion role. *Journal of Small Business and Enterprise Development*, Vol. 24 No. 1, pp. 68-87.

Hair J.F., Sarstedt, M., Hopkins, L. and Kuppelwieser, G.V. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European Business Review*, Vol. 26 No. 2, pp. 106-121.

Hair, J., Hollingsworth, C.L., Randolph, A.B. and Chong, A.Y.L. (2017). An updated and expanded assessment of PLS-SEM in information systems research. *Industrial Management & Data Systems*, Vol. 117 No. 3, pp. 442-458.

Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E. and Tatham, R.L. (2006). *Multivariate data analysis* (6th edition.). Pearson Prentice Hall, New York, NY.

He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., and Tian, X. (2019). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital*. Vol. 21 No. 2, pp. 203-213.

Henseler, J., Dijkstra, T. K., Sarstedt, M., Ringle, C. M., Diamantopoulos, A., Straub, D. W., Ketchen, D. J., Hair, J. F., Hult, G. T. M. and Calantone, R. J. (2014). Common Beliefs and Reality about Partial Least Squares: Comments on Rönkkö & Evermann (2013), *Organizational Research Methods*, Vol. 17 No. 2, pp. 182-209.

Henseler, J., Hubona, G. and Ray, P.A. (2016). Using PLS path modeling in new technology research: updated guidelines. *Industrial Management & Data Systems*, Vol. 116 No. 1, pp. 2-20.

Henseler, J., Hubona, G.S. and Ray, P.A. (2017). 'Partial least squares path modeling: updated guidelines', Latan, H. and Noonan, R. (Eds), *Partial Least Squares Structural Equation Modeling: Basic Concepts, Methodological Issues and Applications*, Springer, Heidelberg, pp. 19-39.

Henseler, J., Ringle, C.M. and Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the academy of marketing science*, Vol. 43 No. 1, pp. 115-135.

Hilary, G., Segal, B. and Zhang, M.H. (2016). 'Cyber-Risk Disclosure: Who Cares?' (October 14, 2016). Georgetown McDonough School of Business Research Paper No. 2852519, available at: http://dx.doi.org/10.2139/ssrn.2852519 (accessed 27 September 2021)

Hu, L.T. and Bentler, P. M. (1998). Fit Indices in Covariance Structure Modeling: Sensitivity to Underparameterized Model Misspecification, *Psychological Methods*, Vol. 3 No. 4, pp. 424-453.

Jamilov, R., Rey, H. and Tahoun, A. (2021), 'The anatomy of cyber risk', Working paper No. w28906, USA National Bureau of Economic Research, June 2021.

Kamiya, S., Kang, J.K., Kim, J., Milidonis, A. and Stulz, R.M. (2018). 'What is the Impact of Successful Cyberattacks on Target Firms?' Fisher College of Business Working Paper No. 2018-03-004, available at: SSRN, https://doi.org/10.2139/ssrn.3135514 (accessed 27 September 2021)

Lallie, H.S., Shepherd, L.A., Nurse, J.R.C., Erola, A., Epiphaniou, G.M., Maple, C. and Bellekens, X. (2021). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. *Computers & Security,* Vol. 105, pp. 1–20.

Lam, L.W. (2012). Impact of competitiveness on salespeople's commitment and performance. *Journal of Business Research*, Vol. 65 No. 9, pp. 1328-1334.

Linkov, I. and Kott, A. (2019). 'Fundamental Concepts of Cyber Resilience: Introduction and Overview', A. Kott, A. and I. Linkov, I. (Eds), *Cyber Resilience of Systems and Networks,* Springer International Publishing, New York, NY, pp. 1–25.

Miron, W. and Muita, K. (2014). Technology Innovation Management Review Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure, *Technology Innovation Management Review*, Vol. 4, pp. 33–39.

Moore, T., Dynes, S., and Chang, F. R. (2015). 'Identifying how firms manage cybersecurity investment',. *Southern Methodist University Blog*, available at: http://blog.smu.edu/research/files/2015/10/SMU-IBM.pdf (accessed 14 December 2015-12-14).

New Zealand. National Cyber Security Centre. (2019). 'Charting Your Course: Cyber Security Governance'. available at: https://www.ncsc.govt.nz/guidance/charting-your-course-cyber-security-governance/ (accessed 28 September 2021)

Newman, L. H. (2020). ‘Schools already struggled with cybersecurity. Then came COVID-19’. Condé Nast, available at: https://arstechnica.com/tech-policy/2020/07/schools-already-struggled-with-cybersecurity-then-came-covid-19/ (accessed 28 September 2021)

Nicola, M., Alsafi, Z., Sohrabi, C., Kerwan, A., Al-Jabir, A., Iosifidis, C., Agha, M. and Agha, R. (2020). The socio-economic implications of the coronavirus pandemic (COVID-19): A review, *International Journal of Surgery*, Vol. 78, pp. 185–193.

Noguchi, M. and Ueda, H. (2017). An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures. *NEC Technical Journal*, Vol. 12 No. 2, pp. 19-24.

Nolan, C., Lawyer, G. and Dodd, R.M. (2019). Cybersecurity: today’s most pressing governance issue. *Journal of Cyber Policy*, Vol. 4 No. 3, pp. 425–441.

O'Neill, P.H. (2020). ‘A patient has died after ransomware hackers hit a German Hospital’. MIT Technology Review. available at: https://www.technologyreview.com/2020/09/18/1008582/a-patient-has-died-after-ransomware-hackers-hit-a-german-hospital/ (accessed 28 September 2021)

Pfleeger, S.L. and Caputo, D.D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*. Vol. 31 No. 4, pp. 597–611.

Renaud, K., Von Solms, B. and Von Solms, R. (2019) ‘How does intellectual capital align with cyber security?’, *Journal of Intellectual Capital*, Vol. 20 No. 5, pp. 621–641. doi: 10.1108/JIC-04-2019-0079.

Rigdon, E.E. (2016). Choosing PLS path modeling as analytical method in European management research: A realist perspective, *European Management Journal*, Vol. 34 No. 6, pp. 598–605.

Rigdon, E.E., Sarstedt, M. and Ringle, C. M. (2017). On Comparing Results from CB-SEM and PLS-SEM: Five Perspectives and Five Recommendations. *Marketing ZFP*, Vol. 39 No. 3, pp. 4–16.

Rosati, P., Deeney, P., Cummins, M., Van Der Werff, L. and Lynn, T. (2019). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in International Business and Finance*, Vol. 47, pp. 458–469.

Rothrock, R.A., Kaplan, J. and Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review*, Vol. 59 No. 2, pp. 12-15.

Sallos, M.P., Garcia-Perez, A., Bedford, D. and Orlando, B. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. *Journal of Intellectual Capital*, Vol. 20 No. 4, pp. 581-597.

Slade, R. (2021). *Cybersecurity Lessons from CoVID-19*. CRC Press, New York, NY.

Spanos, G. and Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers and Security*, Vol. 58, pp. 216–229.

Streukens, S. and Leroi-Werelds, S. (2016). Bootstrapping and PLS-SEM: A step-by-step guide to get more out of your bootstrap results. *European Management Journal*, Vol. 34 No. 6, pp. 618-632.

Sun, L., Srivastava, R.P and Mock, T.J. (2006). An information systems security risk assessment model under the Dempster-Shafer Theory of Belief Functions. *Journal of Management Information Systems*, Vol. 22 No. 4, pp. 109-142.

United Kingdom. British Standards Institute (BSI). (2018). 'Cyber risk and resilience. Guidance for the governing body and executive management. BS 31111:2018'., available at: https://www.britishstandard.org.uk/pub/bs-311112018-9780580944826.aspx (accessed 28 September 2021)

United Kingdom. Department for Digital, Culture, Media and Sport (DCMS). (2021). 'Cyber Security Breaches Survey 2021'. , available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021 (accessed 28 September 2021)

USA. National Institute of Standards and Technology (NIST). (2018). 'Framework for Improving Critical Infrastructure Cybersecurity v1.1', available at: https://www.nist.gov/cyberframework (accessed 28 September 2021)

Venturini, S. and Mehmetoglu, M. (2017). PLSSEM: A stata package for structural equation modeling with partial least squares. *Journal of Statistical Software*, Vol. 88 No. 8, pp. 1–35.

Wagner, D. and Disparte, D. (2016). *Global risk agility and decision making: Organizational resilience in the era of man-made risk*. Palgrave Macmillan, London.

Weill, P., Apel, T., Werner, S.L. and Banner, J.S. (2019). It Pays to Have a Digitally Savvy Board. *MIT Sloan Management Review*. Vol. 60 No. 3, pp. 41-45.

Wiggen, J. (2020). 'The impact of COVID-19 on cyber crime and state-sponsored cyber activities',. Konrad Adenauer Foundation, available at: https://www.kas.de/en/analysen-und-argumente/detail/-/content/die-auswirkungen-von-covid-19-auf-cyberkriminalitaet-und-staatliche-cyberaktivitaeten (accessed 28 September 2021)

Wirth, A. (2020). Cyberinsights: COVID-19 and What It Means for Cybersecurity. *Biomedical Instrumentation & Technology*, Vol. 54 No. 3, pp. 216–219.

Zaboeva, C. and Frydrych, M. (2020). 'IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain',. Security Intelligence, available at: . https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/ (accessed [8 January 2021)]

Appendix A. Questionnaire items

Focus: general, foundational elements of a cybersecurity framework. Key, common elements across cybersecurity frameworks. (1= high disagreement and 5= high agreement)
DECT: Our organisation has effective measures in place for the detection, mitigation and response to cyber security incidents POLY: Our organisation's information security policy includes measures related to cyber security REVW: Our organisation regularly reviews our cyber crisis or incident response plan *Sources*: UK's Cyber Essentials scheme; ISO 27000 family of standards (ISO/IEC 2018); NIST cybersecurity framework (NIST 2018)
Capability: higher-order specifications, characteristics, and good practices associated with cybersecurity performance (1= high disagreement and 5= high agreement)
DIGT: Our management board has a sufficient understanding of the threats digital technologies currently pose to our organisation MECH: Our organisation has effective mechanisms in place for the production, analysis and utilisation of cyber intelligence (i.e. identification of risks and threats) ASST: Our organisation has a sufficient understanding of our key digital assets and services, and the interdependencies between them COMM: In the event of a cyber security incident, our organisation has efficient mechanisms in place for external communication with the potentially affected parties PART: Our organisation is involved in a programme or external partnership for the sharing of cyber security information, expertise, technology and/or resources, as and when required *Sources*: Rothrock et al. 2018; Nolan et al. 2019; NIST 2018.
Resilience: organisation's ability to absorb and overcome successful cyberattacks while maintaining core function (1= high disagreement and 5= high agreement)
LEGS: Our organisation's information security policy is updated as required to comply with cyber security legislation BUDG: The budget our organisation has allocated to cyber security is sufficient CRIT: Our organisation has effective measures in place to remain operational even if we lose access to a critical digital asset (e.g. a particular database or application) *Source*: Bjorck *et al*. 2015; Rothrock *et al*. 2018.
Prep: themes surrounding training and preparation both for executives and operational employees (1= high disagreement and 5= high agreement)
TOPP: Cyber security is one of the top priorities for our management board MEAS: Our organisation regularly measures the extent to which cyber security is embedded in our operations TAIN: Our organisation's training and awareness programme on cyber security for employees is effective TABT: Our management board regularly participate in cyber security exercises such as table-top and cyber wargames *Source*: Weill et al. 2019.
Risk: perception of changes in the risk climate as a result of the COVID-19 pandemic. (1= high disagreement and 5= high agreement)
DATB: The risk of a data breach for our organisation has increased during the current COVID-19 crisis CYBS: The current COVID-19 crisis has increased the cyber security risk for our organisation
Cyber investment: perception of changes in investment patterns as a result of the COVID-19 pandemic. (1= high disagreement and 5= high agreement)
INVEST: Our organisation's investment in cyber security has changed as a result of the current COVID-19 crisis