Enhancing Decision-Making about Cyber Risk: Perspectives from Maritime Security

Kristen Kuhn (BSc. MSc.)

Coventry University

Thesis presented for the degree of Doctor of Philosophy (PhD)
November 23, 2022

Declaration

All sentences or passages quoted in this document from other people's work have been specifically acknowledged by clear cross-referencing to author, work and page(s). Any illustrations that are not the work of the author have been used with the explicit permission of the originator and are specifically acknowledged. I understand that failure to do this amounts to plagiarism and will be considered grounds for failure.

Kristen Kuhn

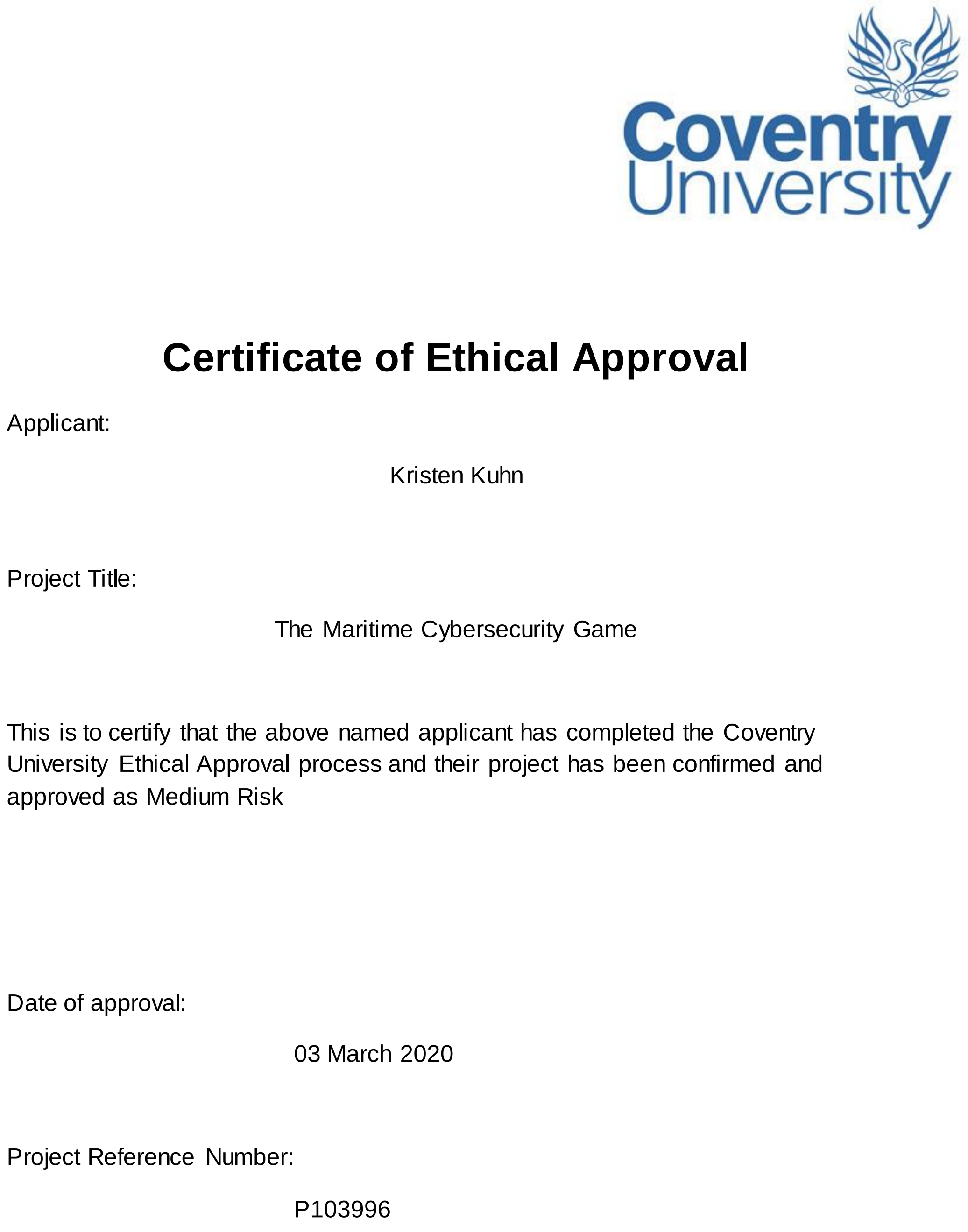
Kristen Kuhn
November 23, 2022

Certificate of Ethical Approval

Applicant:	Kristen Kuhn
Project Title:	The Cybersecurity Simulation Exercise

This is to certify that the above named applicant has completed the Coventry University Ethical Approval process and their project has been confirmed and approved as Medium Risk

Date of approval:	15 Dec 2020
Project Reference Number:	P116179



Certificate of Ethical Approval

Applicant:

Kristen Kuhn

Project Title:

The Maritime Cybersecurity Game

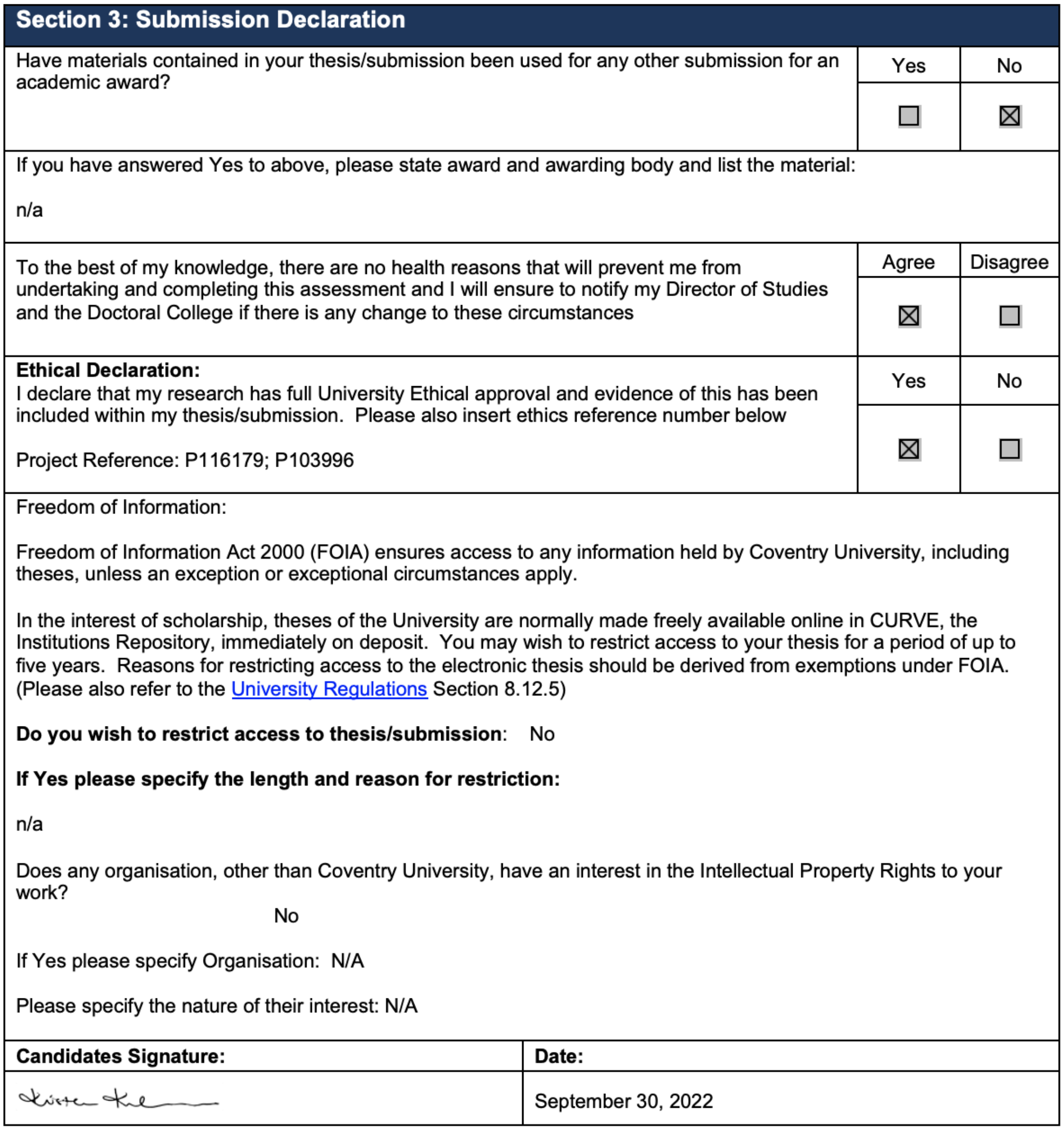
This is to certify that the above named applicant has completed the Coventry University Ethical Approval process and their project has been confirmed and approved as Medium Risk

Date of approval:

03 March 2020

Project Reference Number:

P103996



Section 3: Submission Declaration

	Yes	No
Have materials contained in your thesis/submission been used for any other submission for an academic award?	☐	☒

If you have answered Yes to above, please state award and awarding body and list the material:

n/a

	Agree	Disagree
To the best of my knowledge, there are no health reasons that will prevent me from undertaking and completing this assessment and I will ensure to notify my Director of Studies and the Doctoral College if there is any change to these circumstances	☒	☐

	Yes	No
Ethical Declaration: I declare that my research has full University Ethical approval and evidence of this has been included within my thesis/submission. Please also insert ethics reference number below Project Reference: P116179; P103996	☒	☐

Freedom of Information:

Freedom of Information Act 2000 (FOIA) ensures access to any information held by Coventry University, including theses, unless an exception or exceptional circumstances apply.

In the interest of scholarship, theses of the University are normally made freely available online in CURVE, the Institutions Repository, immediately on deposit. You may wish to restrict access to your thesis for a period of up to five years. Reasons for restricting access to the electronic thesis should be derived from exemptions under FOIA. (Please also refer to the University Regulations Section 8.12.5)

Do you wish to restrict access to thesis/submission: No

If Yes please specify the length and reason for restriction:

n/a

Does any organisation, other than Coventry University, have an interest in the Intellectual Property Rights to your work?
No

If Yes please specify Organisation: N/A

Please specify the nature of their interest: N/A

Candidates Signature:	**Date:**
	September 30, 2022

Abstract

Cyber threats to maritime organisations are becoming increasingly prominent. Given the significant likely impacts and the high-profile media attention surrounding previous attacks, it is unsurprising that leaders within maritime organisations are motivated to engage with cyber risks. This has catalysed the development of new cybersecurity guidance, however this focus on the organisational side has not been met with the same balance within scholarly discourse, with most research positioned within the technical aspects of cybersecurity. As limited research exists examining decision-making at senior leadership levels, this thesis seeks to address this gap by critically exploring the potentiality of simulation-based approaches for enabling more effective decision support at this level. The literature review develops an understanding of the risks, impacts and challenges influencing cybersecurity decision-making in the maritime domain. It also identifies game-based simulation as the most effective method for simulation-based approaches in cybersecurity. The research develops, tests, and applies two scenario-driven exercises for executive decision-makers which offers insights about cybersecurity risks and decision-making processes. Through these findings, it establishes the potentiality of game-based learning for raising awareness of cyber risks at the senior executive level. A key implication includes building on existing literature to establish decision-making as a key factor in what makes executive decision-makers analyse cyber risk and respond to cybersecurity incidents effectively. By designing exercises that create a safe space environment, it also provides evidence to the senior leadership of such organisations, from which they can understand the potential eventualities of a cyber attack in the absence of an attack actually happening.

Keywords— Cybersecurity, Decision-making, Risk perception, Maritime

Acknowledgements

I would like to express my sincere gratitude to my supervisors Professor David McIlhatton, Professor Rachel Monaghan, and Professor Siraj Shaikh for their guidance, patience and support during my PhD study.

Thank you to my collaborators for the many discussions that challenged me on this topic. I would also like to thank those who took the time to facilitate and participate in this research, for their insights and appreciation of the impact this research can have in enhancing decision-making about cyber risk.

Finally, I wish to thank my family, friends and colleagues for their encouragement which kept me going. Most thanks to Alvaro for his never-failing sympathy and counsel that saw me through this PhD from start to finish. And thank you to Eva who simply is a better person than I, even though she is a dog.

Acronyms

AOS Arden Ocean Shipping

BIMCO Baltic and International Maritime Council

BMS building management system

CEOs Chief Executive Officers

CIOs Chief Information Officers

CIP Inter-American Committee on Ports

COE-DAT The Centre of Excellence Defence Against Terrorism

COVID-19 Coronavirus disease

CR4B Cyber Readiness for Boards

ENISA European Union Agency for Network and Information Security

GDPR General Data Protection Regulation

GPSs global positioning systems

ICT Information and Communications Technology

IMO International Maritime Organisation

IoT Internet of Things

IT information technology

KIPS Kaspersky Interactive Protection Simulation

NATO North Atlantic Treaty Organization

NCSC National Cyber Security Centre

NIST National Institute of Standards and Technology

OAS Organisation of American States

RF ID radio frequency ID

UN United Nations

Contents

List of Figures

List of Tables

Chapter 1
Introduction

This Critical Overview Document (the ‘thesis’) draws together a coherent body of inter-related research, published between 2019 and 2022, on maritime cybersecurity and enhancing decision-making about cyber risk. It develops an understanding of the risks, impacts and other associated challenges influencing cybersecurity decision-making in the maritime domain by developing, testing and applying scenario-driven exercises for executive decision-makers to understand cybersecurity risks and decision-making processes. It also analyses the most effective methods for simulation-based approaches in cybersecurity. The outcome is the established potentiality of game-based learning for raising awareness of cyber risks at the senior executive level.

1.1 Background

Cyber threats to maritime organisations are becoming increasingly prominent. This is unsurprising given that 90 percent of world trade is based within the maritime global supply chain (International Chamber of Shipping, 2020) which includes shipping, distribution of goods and services, and the integration of trans-national companies’ global network. Evidence demonstrates that as organisations, governments and citizens become more reliant on digital technology to function (National Cyber Security Centre, 2019), attackers are increasingly moving away from analogous threat vectors to exposing and exploiting vulnerabilities within digital environments (Pearlson et al., 2021). The maritime domain comprises a significant number of organisations related to transport, defence, energy, fishing, and leisure- all of which are intrinsically dependent on digital technology to function. These technologies, including global positioning systems (GPSs), satellite technology and other connected infrastructures, are collectively known as Information and Communications Technology (ICT), and are integral to the ability of organisations to operate effectively and efficiently at the international level. As a result of the dependence on these technologies and the inter-dependencies that exist within the global maritime supply chain, an environment exists whereby significant vulnerabilities arise as the exploitation of vulnerabilities in one company may have significant cascading effects, intentional and unintentional consequences for other suppliers and organisations (Grasso Macola, 2020) which may impair their function and, in extreme cases, paralyse the global economy (Greenberg, 2018).

Despite this, many organisations must balance the risks and opportunities that ICT provides for maritime organisations. Advances in digitisation and automation (Tam and Jones, 2019) are becoming mainstream considerations within such organisations. A move towards using technology such as satellite communications has provided shipping organisations with the ability to provide their customers with real-time tracking information (VesselFinder, 2022). The introduction of radio frequency ID (RF ID) technology has also allowed maritime organisations to track the movement of their assets on land and sea, as well as manage the distribution of them more effectively and efficiently. Furthermore, the development of autonomous technology has allowed organisations to reduce risk in relation to considerations such as health and safety.

Despite these significant and attractive opportunities for maritime organisations, the move towards digitisation and automation carries significant risks. According to the Cambridge Centre for Risk Studies (Cambridge Centre for Risk Studies, 2019), these risks include those related to financial, geopolitical, governance, environmental, and also social and technology risks. Many of these risks emerge and are exemplified by issues including cybersecurity, as attackers seek to expose and exploit the vulnerabilities of these organisations.

In example, at the international level, the World Economic Forum's Global Risks Report 2020 (World Economic Forum, 2020) detailed that cybersecurity was now an existential risk to organisations globally. In a similar vein, the International Maritime Organisation (IMO) (International Maritime Organization, 2017) and international shipping associations such as the Baltic and International Maritime Council (BIMCO) (BIMCO, 2018) have highlighted cybersecurity as significant challenges for their industry. At the organisational level, cyber risk is now widely regarded as a top organisational risk (Antonucci, 2017), but the problem is that most organisations have not received the type and level of support required to incorporate cyber into their risk portfolios.

In 2017, the Not-Peta ransomware attack on Moller-Maersk, the world's largest container shipping line, disrupted their operations for two weeks, resulted in a 20 percent reduction in shipping volume, caused $300 million in direct economic damage and led to a $8.4 billion loss to shareholders (Cyberhedge, 2020). This destabilising attack underscores the importance of cybersecurity and has since become legendary in the maritime sector (Kuhn et al., 2021a).

More recently, and in the last two years alone, maritime organisations have experienced at least eight (Kuhn et al., 2021a) high-impact cyber attacks that have evolutionised operational and strategic approaches in cybersecurity. In July, 2019, the UK tanker *Sterna Impero* was victim to GPS spoofing that sent it off course into Iranian waters, where it was subsequently seized and its 23 crew members arrested (Wiese Bockmann, 2019). In January, 2020, logistics giant Toll Group suffered a ransomware attack that shutdown systems, leading to operational delays and disruptions on land and at sea (Wingrove, 2020). In April, 2020, shipping giant MSC suffered a malware attack that caused network outage at its headquarters (Twining, 2020). In June, 2020, Toll Group suffered another ransomware attack which led to stolen information and the shutdown of information technology (IT) systems (Wingrove, 2020). In the same month, a malware attack on the Shaid Rajee Port in Iran crashed the facility computer systems and caused transport chaos which lasted days (Al Jazeera Media Network, 2020). In September, 2020, shipping line CMA CGM suffered a ransomware attack which forced the container line to shutdown its network (Shen and Baker, 2020) and a US tug boat endured a phishing attack (Grasso Macola, 2020). In October, 2020, malware took down the IMO website and intranet, forcing the United Nations (UN) organisation to shutdown key systems at a time when they were launching new cybersecurity guidelines that require shipping to improve digital security (Konrad, 2020).

Whether intentional or unintentional, maritime cybersecurity incidents have had and will likely continue to have catastrophic consequences. In previous research (Konrad, 2020), a detailing of the *"unimaginable"* damage that would occur if hackers entered into the autopilot systems of an entire global fleet of vessels demonstrates clearly the significant and impactful challenges that a failure to understand, manage and mitigate cybersecurity risks may have for organisations. Other reseach (Daffron et al., 2019) developed and tested a scenario that helped understand the potential damage that a computer virus infecting 15 major ports across Asia Pacific would have and calculated an economic loss upwards of $110 billion.

Given the significant likely impacts and the high-profile media attention surrounding previous attacks, it is unsurprising that leaders within maritime organisations are motivated to engage with cyber risks. This motivation has catalysed the development of new guidance for improving cybersecurity in organisations, albeit most of this has focused on operational cybersecurity. In example, in 2018 the US National Institute of Standards and Technology (NIST) published the NIST Cybersecurity Framework (National Institute of Standards and Technology, 2018) for improving cybersecurity of critical infrastructure. In the same year, the EU General Data Protection Regulation (GDPR) (European Commission, 2018) came into force and BIMCO released The Guidelines on Cyber Security Onboard Ships (BIMCO, 2018). In 2020, the UK National Cyber Security Centre (NCSC) published The Cyber Security Toolkit for Boards (National Cyber Security Centre, 2019), which is unique in that it encourages cybersecurity discussions between technical experts and boards, which refers to groups of *"executives"* who make decisions to drive an organisation's direction and strategy.

This focus on the organisational side has, however, not been met with the same balance within this scholarly discourse, with most research positioned within the technical aspects of cybersecurity. A more limited body of knowledge is evident for cybersecurity decision-making at the senior leadership level. Much of the research that has been conducted at the leadership level is driven by a perceived need to improve the technical understanding of decision-makers, with other research (Jalali et al., 2019) focusing more broadly on decision-making and biases in cybersecurity capability development. In their research, they found experienced managers do not outperform inexperienced individuals in building cybersecurity capabilities, and one outcome from the research was that proactive decision-making can be taught more effectively through an iterative learning process such as a simulation of potential real world incidents.

Where cybersecurity research has investigated high-level decisions about how the security of organisations and systems are managed, it has mainly focused at the level of security managers (Moore et al., 2015) and not reached the level of executive decision-makers interacting with other functions at the highest level of an organisation. In addition, limited empirical evidence has emerged helping industry at the board level to understand the most appropriate methods and approaches for decision-making in relation to cybersecurity issues. As computer technology and networked systems increasingly become part of normal business operations (Pallas, 2009), there are calls for cybersecurity to be recognised as a top-level, board responsibility, given its nature and that it *"will impact all aspects of a business including strategy, business development, supply chain, staff and customer experience"* (Horne, 2017).

As limited research exists examining decision-making at senior leadership levels, this thesis seeks to address this gap by critically exploring the potentiality of simulation-based approaches for enabling more effective decision support at this level. As a consequence of this shortcoming in the literature, the senior leadership of such organisations, such as the board of directors or trustees, have limited evidence from which they can understand the potential intended and unintended consequences of a cyber attack in the absence of an attack actually happening. The research presented in this thesis has been designed in a way that provides a safe space environment for senior leadership to understand such eventualities.

While the senior leadership of organisations may take many forms, this research focuses on governance-related decisions involving multiple decision-makers who are challenged by securing the organisation on one hand and not compromising the organisation's ability to operate as it normally would for any extended period.

1.1.1 Contribution

The original contribution of this thesis is threefold. First, it provides new approaches, evidence and insights for closing the gap in extant literature, whereby a review of the extant literature base has not identified a body of knowledge focused on cybersecurity decision-making at the senior leadership level utilising scenario-based approaches. Second, it researches and develops methods and approaches for supporting decision-making in the context of cybersecurity incidents, cyber risks and consequently cyber readiness. Third, this thesis tests and validates these methods and approaches, highlighting the potentiality or otherwise of simulation-based approaches for enhancing decision-making.

The autobiographical context for this thesis is introduced in Section 1.2, followed by the aim and supporting objectives in Section 1.3. A chronology of research outputs is presented in Section 1.4. Subsequently, the approach and structure for the research are presented in Section 1.5 and Section 1.6, which allows for the examination of the theoretical components which lay the groundwork for the empirical investigation.

1.2 Autobiographical Context

I was introduced to the maritime sector by Jorge Duran, Chief of the Secretariat at the Inter-American Committee on Ports (CIP) while working at the Organisation of American States (OAS). For someone from Michigan, which has no ocean, maritime seems an odd specialisation- yet it combines many of my interests: international relations, technology, and security. Following this inclination, I moved to Barcelona in 2015 with a full scholarship from the Spanish defence agency INDRA to undertake a Master's in International Security. My dissertation was on port automation and cybersecurity. Incidentally, I met a professor who connected me with the International Dockworkers Council, where I was hired on as Head of Secretariat. In this role, I visited ports around the world and took part in policy dialogues, including at the European Parliament and with the EU Commissioner of Transport. Thus, I was able to conduct research and simultaneously work in the maritime sector. Motivated to further my education, in 2019 I reached out to Prof. Siraj Shaikh and we found a shared interest: I wanted a PhD and he sought a researcher on the Cyber Readiness for Boards (CR4B) project, a two-year position I accepted. We found that I was suited to the role as I have worked closely with Chief

Executive Officers (CEOs), which provided me with unique experience for the project.

My rationale has been clear since September 2019 and I have stuck within the scope of my work and produced independent outputs that are stand-alone, high-level and relevant contributions to the field. The pursuit of a PhD by publication not only complemented my work at Coventry University, but strengthened it and vice-versa. The research journey occurred in a manner which allowed me to build a stronger base of knowledge, and then apply it in the creation of cybersecurity decision-making exercises. It also captured the inter-relationship between the outputs, whereby an in-depth understanding of the field was achieved before a new approach was developed. Moreover, during the process of preparing this thesis, I was able to appreciate the value of research methods and critical reflections as integral factors that govern my future research and practice.

1.3 Aim and Research Objectives

The principal aim of this research is to develop approaches for enhancing the understanding of cybersecurity risk at the senior leadership level in organisations. The purpose of this research is not to develop a tool for helping leaders make decisions relating to cybersecurity risks; instead it is to research, develop and test methods that help raise awareness of cybersecurity risks at the leadership level and the potential impact of their decision-making for countering and mitigate these risks. In fulfilling the aim, four objectives are utilised to develop knowledge and understanding of simulating cybersecurity risks:

1. To develop an understanding of the risks, impacts and other associated challenges influencing cybersecurity decision-making in the maritime domain;

2. To analyse the most effective methods for simulation-based approaches in cybersecurity;

3. To develop, test and apply scenario-driven exercises for executive decision-makers to understand cybersecurity risks and decision-making processes;

4. To establish the potentiality of game-based learning for raising awareness of cyber risks at the senior executive level.

1.4 Output Chronology

This thesis is comprised of seven outputs from research on maritime cybersecurity and enhancing decision-making about cyber risk, undertaken between 2019 and 2022, whilst employed as a researcher at Coventry University. To ensure the development of a coherent narrative and argument which best addresses the research aim and objectives, a 'Logic of Research Outputs' was developed in Table 1 (page 19) to 'phase' the outputs appropriately. In doing so, it should be noted that the outputs are sequenced in non-chronological order; rather, they are ordered in the following way:

- **Output 1:** Kuhn, K., Kipkech, J. & Shaikh, S. (2021) **Maritime Ports and Cybersecurity.** In *Maritime Transport and ITS Solutions in Port Logistics*, pages 37–67. Institution of Engineering and Technology. ISBN: 978-1-83953-086-9. Peer-reviewed book chapter.

- **Output 2:** Kipkech, J., Kuhn, K. & Shaikh, S. (2022) **Cyber Security and Disruptive Technologies.** In *Routledge Handbook of Maritime Security*, pages 214-226. Routledge. ISBN: 978-0367430641. Peer-reviewed book chapter.

- **Output 3:** Kuhn, K., Vasudevan, S. & Carr, M. (2020) **Cyber Insurance and Risk Management: Challenges and Opportunities.** *Research Institute for Sociotechnical Cyber Security.* https://www.riscs.org.uk/cyber-insurance/. Report.

- **Output 4:** Hussain, A., Kuhn, K. & Shaikh, S. (2020) **Games for Cybersecurity Decision-making.** In *Fang, X. (eds) HCI in Games. HCII 2020. Lecture Notes in Computer Science, vol 12211,* Springer. DOI: 10.1007/978-3-030-50164-8_30. Peer-reviewed conference proceeding.

- **Output 5:** Kuhn, K., Bicakci, S. & Shaikh, S. (2020) **Maritime Cyber Risk Perception and Response.** In *4th NMIOTC Conference on Cybersecurity in the Maritime Domain*, pages In–Press. https://nmiotc.nato.int/pressreleases/4th-cyber-security-conference-in-maritime-domain/. Peer-reviewed conference proceeding.

- **Output 6:** Kuhn, K. Bicakci, S. & Shaikh, S. (2021) **COVID-19 Digitisation in Maritime: Understanding Cyber Risks.** *WMU Journal of Maritime Affairs,* 20(2), 193–214 . DOI: 10.1007/s13437-021-00235-1. Peer-reviewed journal article.

- **Output 7:** Parkin, S., Kuhn, K. & Shaikh S. (2021) **Scenario-Driven Assessment of Cyber Risk Perception at the Security Executive Level.** In *Workshop on Usable Security and Privacy*, pages In–Press. http://www.usablesecurity.net/USEC/usec21/papers/usec2021_Simon_Parkin.pdf. Peer-reviewed conference proceeding.

Table 1 (page 19) illustrates how the Logic of Research Outputs sequences the outputs to best address the research aim and objectives. A full justification is then provided in the subsequent chapter "Research Journey" (Chapter 5).

1.5 Research Methodology

The research outputs focus on developing exercises to improve cybersecurity decision-making. This effort aims to assess how cybersecurity and risk are perceived at the top level in organisations. This would ensure alignment of cyber risk management decisions (amidst rapid developments in the technologies of networked, IT-supported business infrastructures) with the view from organisation leadership. The first part of this research is primarily desk-based, with the theoretical aspects focusing on a review of extant literature, current and emerging practice. The second part of this research is experimental, for which the simulation method is employed to develop and implement two cybersecurity decision-making exercises. This method was chosen for a variety of reasons, detailed in Section 1.5.2, including that it promotes experiential learning and systems thinking, facilitates an appropriate research approach which can address the research questions and considers limited participant availability.

To ensure the research aim is addressed and the objectives are achieved, the methodology incorporates a mixed-method approach, which is adopted from a research methodology (Creswell et al., 2003) which includes qualitative and quantitative research methods. The methods employed in this thesis include desk-based research, simulation exercises and content analysis. However, the case-study method approach may also be considered an appropriate method of inquiry, whereby the case-study may be interpreted (Creswell, 2002) as an in-depth process of investigation that incorporates a variety of methods. In line with Creswell et al.'s (2003) work, the qualitative strategy of this thesis focuses on defining the observations, experiences, views and attitudes of executive decision-makers within the context of cybersecurity, by which means research was conducted in line with good qualitative ethical practice. This method includes an introduction, a review of maritime cybersecurity and decision-making, the research approach including analysis of data and results, and a conclusion.

1.5.1 Qualitative Research

The qualitative research approach provides a foundation for structured investigation of descriptive perception (Wisker, 2018). Three research methods associated with qualitative research include in-depth interviews, focus group discussion and observation (Hennink et al., 2020). These methods foster an understanding of a phenomena through the inquiry of varying philosophical assumptions (Creswell, 2009). These assumptions are rooted in the twin paradigms of interpretivism and positivism, including the areas where they intersect-or where qualitative and quantitative research methods mix (Hennink et al., 2020). For example, the content analysis undertaken in this thesis represents an approach to qualitative research with positivist influences; while open questions posed in surveys are an example of quantitative methods that include interpretive elements. In this sense, the mixed-methods approach includes not only three qualitative research methods, but also qualitative methods with some quantitative elements- and vice versa. This approach allows for study that is flexible whilst encouraging an inductive style. In this case, findings include assessing cybersecurity decision-making without saying whether it's good or bad.

The qualitative research approach is appropriate for this thesis as it provides a foundation for structured investigation of descriptive perception (Wisker, 2018), given the research undertaken represents an exploratory investigation in an under-researched area- perceptions of cyber risk at the highest levels of an organisation. Through a mixed-method approach, this thesis employs (to varying degrees) each of the three methods associated with qualitative research: observation, focus group discussion and in-depth interviews (Hennink et al., 2020). The focus of this thesis is on the first two methods, through means of simulation exercises which are both observed and followed up with semi-structured scenario questions which guide discussion. Less emphasis is placed on in-depth interviews, given that the exercises are built around the need to collect a lot of information quickly in a group setting (focus group discussion) and the desire to observe how participants act in controlled social situations. However, the pre-exercise questions may be considered (to a lesser extent) a form of interview and are important to the study as they provide some personal information of participants as well as their experiences (for instance, their technical knowledge of cyber) which allows for results to be contextualised.

As the researcher spent time with participants for the duration of the exercise, qualitative research raises inherent validity considerations including strategic, ethical and personal issues. Creswell (Creswell, 2017) suggests the researcher has additional roles in a study which includes creating a setting whereby the validity of the experiment is not called into dispute. This was the case in this thesis, whereby the researcher assumed 'many hats' during the exercise, including observer, exercise and discussion facilitator, and 'technical expert.' In this way, the participants could ask and receive information on technical questions related to the exercise and scenarios, while the researcher (who was aware of these elements) could omit information that might impact the study, such as disclosing their own bias, values, or personal background in ways that might alter participant perception or game-play. Effort was taken to ensure that any of the considerations that may affect the researcher's perspective on the data or resulting outcomes were considered in publications and and addressed through disclosure (Creswell, 2017).

Other research methods were considered for this thesis, including quantitative methods. However, as the experimental portion of this thesis has not been carried out before and a limited number of participants took part in it (the number of exercises are limited) it would not have been appropriate to use a classic quantitative method, such as statistical analysis, to generate normative findings that are explicitly geared towards evaluation of a broader population, such as level of uncertainty or predictability. While this thesis establishes a new intervention, not enough data is collected for a statistical analysis to be meaningful (the samples are not significant enough). In this sense, this thesis presents and pilots exercises, demonstrating repeatable qualitative methods that can be further validated with greater use (a larger sample has greater significance).

Further, this thesis is not interested in 'rating' participants as their decisions are subjective and they are the expert in the room. Rather, it intends to 'hold a mirror' up to them through interpretive analysis (Hennink et al., 2020), assessing characteristics of their cybersecurity decision-making and offering them the opportunity to reflect on it. Also, as this thesis aims to understand executive decision-making, it is concerned with collective assessment to learn about such processes at the senior leadership level, such as those which occurs on boards. While group dynamics are acknowledged to be present in group decision-making, capturing these dynamics is beyond the scope of this exploratory study. Unless the exercises are well-established and accepted in practice, it does not make sense to go to that level of detail.

Facilitating a summary of existing literature that is both generic and specific in a specialised field of study, as well as critical discussion, literature reviews are a key academic requirement. An organised exploration is conducted to establish a strong underpinning that can support a research study (Creswell, 1994) and its proposed methodology. This includes a description of how the study relates to other academic work, which ensures its originality and relevance in the field. As the purpose of this thesis is to make a significant and original contribution to the field, a literature review exposes gaps and any errors in published research that may then be considered (Wisker, 2007). It confirms that duplication of current works does not occur and provides a justification for the research undertaken. In this thesis, the literature review contextualises the complexity and challenges associated with decision-making about cyber risk in the maritime sector. Further, it explores the role of cybersecurity games in enhancing decision-making and provides a platform from which to critically examine methods to approach cybersecurity decision-making, including a justification of the simulation method, fulfilling Research Objectives 1 and 2 (Section 1.3).

1.5.2 Simulating Cyber Attacks

A simulation is *"the imitation of the operation of a real-world process or system over time"* (Banks et al., 2005). Banks et al. (2005) indicate the importance of simulation, which for the purpose of this research is two-fold. First, it enables the study of internal interactions of a complex system or its subsystems, such as an organisation's response to a cyber incident. Second, simulation can be used to experiment with new designs or policies before implementation, so as to prepare for what might happen; for instance planning incident response. Others (Smith and Elliott, 2007) establish that simulations not only test preparedness, but can *"provide decision-makers with experiential learning"*.

There are various approaches to simulation (Dooley, 2017). Simulation may involve participants that attempt to maximize their fitness functions by interacting with other participants and resources to promote a holistic approach to understanding dependencies and emergent processes among elements in a system (Robbins and Aydede, 2008). Simulation is appropriate for this thesis as the complexity of cyber means that decision-makers have a need for training with focus on such thinking (Jalali et al., 2019).

Simulation also offers the opportunity for the researcher to both observe and later engage with participants. This is important because participant behaviour is determined by embedded schemas which are both action-oriented and interpretive in nature. The advantage here is the ability to frame lines of questioning generated from observation, allowing the participants to provide contextual information that is relevant to the findings at hand, such as insight into their priorities. In this sense, the study can attempt to answer not only the 'how' and 'what' of the questions but also the 'why' behind the answers given. This is not the case in another simulation (Jalali et al., 2019) that studies the effectiveness of cybersecurity decision-making, in which a computer-based model receives participant input but does not have the capacity to consider the 'why' behind it.

This thesis refers to simulations which range over different formats including games and exercises. In referencing games, it refers to games in relation to game-based learning. Previous research (Whitton, 2012) articulates the difficulty in defining the term "game" as definitions depend on the disciplinary background of those who create them. To this effect, the field of gaming is interdisciplinary (Crookall, 2000). Others (Salen and Zimmerman, 2004) define a game as a *"system in which players engage in an artificial conflict, defined by rules, which results in a quantifiable outcome"*. However, this thesis considers that games may or may not have quantifiable outcomes. Similar to exercises, participants need to perform in the roles assigned to them and reflect on their own performance while doing it (Lee et al., 2009). This may lead to greater understanding of potential risks to increase preparedness. In the context of this thesis, a game is therefore defined as the method in which participants engage in decision-making to develop an understanding of cyber risk. Further, while games may be competitive (Haggman, 2019), the researcher felt that the term 'game' could be misleading, whereas participants might infer competition. The simulations presented in this thesis allow maritime cybersecurity decision-makers to test concepts, procedures, systems and tactics in response to a cyber attack. To avoid misconceptions around 'rating' and 'winning', the game-based simulations developed in this thesis are referred to as 'exercises.'

An array of factors must be considered in the shaping of an appropriate methodology, such as participant availability and the research questions. In this case, the intent was to recruit highly–experienced participants who are rare to find. Difficulty in recruiting security managers at this level has been noted elsewhere (Reinfelder et al., 2019), due to their high workload and *"poor reachability."* The simulation approach was selected to conduct the experimental part of this thesis as it allows the researcher to collect lots of information from a group in a short time, and offers participants flexibility. For instance, the developed exercises may be carried out in person or virtually, while facilitating a controlled environment in which to test theories and concepts. This proved important given social distancing protocols during the Coronavirus disease (COVID-19) pandemic.

The simulation approach is informed by the researcher's theoretical perspective and how the data is analysed. The subjective nature of decision-making necessitates a method that allows for the contextualisation of data (the 'why') to be able to assess effectiveness. Balancing a need for both objective and subjective findings, this approach incorporates various research methods (survey analysis, observation, semi-structured interviews and content analysis). The approach allows in-depth investigation which makes it a suitable method for a study focused on decision-making around a specific type of event, such as a cyber incident. The multiple case-study approach (incorporating two simulation exercises) also allows for identification of potential similarities and differences across differing groups, including those based on sector, to enable more robust findings (Stake, 2000).

The approach is also informed by the study rationale (Crotty, 2020) which calls for new tools to build the cybersecurity decision-making capacity of executives. This is accomplished by defining characteristics of decision-making in cybersecurity games and then developing structured, scenario-driven exercises for executives to assess cybersecurity decision-making, in turn fulfilling Research Objectives 3 and 4 (Section 1.3).

While the benefits of simulation are discussed above, the method raises inherent validity considerations as it is challenging to mimic forces that motivate participants' drive to complete a task. It is even harder to mimic potential risks and consequences which inform their decision-making. While game participants are aware that the game is not real, they should behave as they would in the real-life situation that the game emulates. Thus, game designers must take pains to preserve ecological validity. This is especially challenging when designing experiments of security and privacy behaviour as these are not the participant's main goal (Schechter, 2013). To address validity, scenario design in Exercise 2 (Parkin et al., 2021) was informed by known cybersecurity incidents that affected organisations. A similar approach has been used to study security analysts (M'manga, 2020). As simulation has been explored in depth, including benefits and possible limitations, this thesis will therefore address any possible conflicting methodological issues.

1.6 Research Design

Each of the research outputs deliver on the objectives of this thesis, as seen in Table 1 (page 19). In the context of fulfilling Objective 1, the research examines cyber attacks in the maritime domain, looking first at ports (Output 1) and then at vessels (Output 2). The research also investigates cyber-risk management strategies to enhance organisational preparedness, including cyber insurance (Output 3). Collectively, this builds a theoretical and conceptual framework which reflects the first research stage. It constructs context by demonstrating the growth of cyber risk in the maritime sector due to increased digitalisation. This sets the stage for introducing games as a tool to address the need for improved cyber risk assessment and, ultimately, underpins the empirical study.

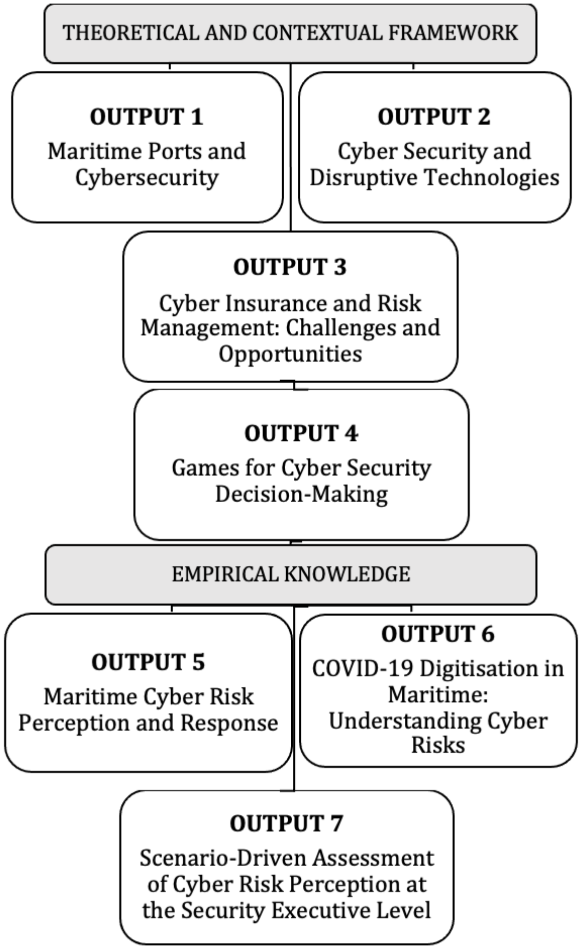
With the aim of addressing Objective 2, the research examines cybersecurity games as a method for simulation-based approaches to enhance cybersecurity decision-making (Output 4). Through analysis of the data-set, a qualitative evaluation criteria to assess such games for decision-making is developed- through which alignment to this criteria offers insights to inform the design of new games. This paves the way for the development of exercises and, as to research stages, marks a shift from theoretical conceptualisation to analysis and findings, as the motivation for the preferred methodological approach (simulation) is established.

With the aim of addressing Objective 3, the research develops two exercises for executive decision-makers to assess cybersecurity decision-making. In terms of research stages, these reflect analysis and findings which focuses on empirical data collection and results, whereby the exercises are designed, implemented and analysed to produce key findings. This thesis first develops a cybersecurity decision-making exercise to assess cyber risk perception (Output 5-6). Using scenarios that range over maritime cyber incidents, this exercise examines the cyber risk perception of a group according to their previous work experience and technical expertise. Assessment of cyber risk perception was done by calibrating group risk. From this, the study explores collective risk perception—tendencies which characterise organisational security culture. It discusses implications for practice and suggests that collective risk perception is a key aspect of decision-making.

This research then develops a second cybersecurity decision-making exercise for executive decision-makers (Output 7). This exercise includes a new methodology which makes use of attack categorisation (Table 8, page 43) and risk categorisation (Table 9, page 45) to provide guidance on scenario design and escalation. These mechanisms allow for the use of narrative hints on the nature of associated risks, stakeholders involved, and non-technical complexities. Such categorisation is also employed as a means of assessment. This underlies a structure to the scenarios as a novel approach to capturing decision-maker insights, providing the potential for bench-marking across groups and sectors (as seen elsewhere in the development of tabletop cybersecurity games (Shreeve et al., 2020)). Further, in terms of the perception of wider business risks, this thesis found the *Cambridge Taxonomy of Business Risks* (Cambridge Centre for Risk Studies, 2019) offers a particular value for structured understanding of business risks, factoring in societal, environmental and geopolitical risks as above and beyond risks internal to the organisation. It demonstrates that wider risks are considered by decision-makers when faced with a cyber incident.

In the context of fulfilling Research Objective 4, the research establishes the potentiality of game-based learning for raising awareness of cyber risks at the senior executive level, reflected in the key research findings (Output 4-7). This encompasses the final research stage of evaluation, which includes conclusions from key research findings, reflections on the contribution and potential directions for future research.

Table 1: *Overall research design*

RESEARCH STAGES	RESEARCH OBJECTIVES	LOGIC OF RESEARCH OUTPUTS
THEORIES AND CONCEPTS Literature Review	**OBJECTIVE 1** To develop an understanding of the risks, impacts and other associated challenges influencing cybersecurity decision-making in the maritime domain	
Methods for Simulation	**OBJECTIVE 2** To analyse the most effective methods for simulation-based approaches in cybersecurity	
ANALYSIS AND FINDINGS	**OBJECTIVE 3** To develop, test and apply scenario-driven exercises for executive decision-makers to understand cybersecurity risks and decision-making processes	
EVALUATION Conclusions from research findings Further research	**OBJECTIVE 4** to establish the potentiality of game-based learning for raising awareness of cyber risks at the senior executive level	

THEORETICAL AND CONTEXTUAL FRAMEWORK
OUTPUT 1
Maritime Ports and Cybersecurity
OUTPUT 2
Cyber Security and Disruptive Technologies
OUTPUT 3
Cyber Insurance and Risk Management: Challenges and Opportunities
OUTPUT 4
Games for Cyber Security Decision-Making
EMPIRICAL KNOWLEDGE
OUTPUT 5
Maritime Cyber Risk Perception and Response
OUTPUT 6
COVID-19 Digitisation in Maritime: Understanding Cyber Risks
OUTPUT 7
Scenario-Driven Assessment of Cyber Risk Perception at the Security Executive Level

Chapter 2

Maritime Cybersecurity and Decision-making; A Review of Related Work

This chapter relates to Research Objectives 1 and 2, which are to understand the complexity and challenges facing cybersecurity decision-making in the maritime sector (1) and to analyse the most effective methods for simulation-based approaches in cybersecurity (2). Collectively, Outputs 1-4 provide a contextual basis that constructs an understanding that is key for the remaining three Outputs. While the Outputs 1-2 focus on ports (Kuhn et al., 2021b) and vessels (Kipkech et al., 2022), Output 3 focuses on cybersecurity insurance (Kuhn et al., 2020b). Output 4 (Hussain et al., 2020) focuses on cybersecurity and acts as a bridge to Research Objective 3 which focuses on developing, testing and applying scenario-driven exercises.

2.1 Understanding Maritime Cybersecurity Risks

Cyber is becoming prominent in extant literature, where a significant volume of research spans a vast array of topics, including information security (Pallas, 2009), digitisation (Ichimura et al., 2022), and automation (Tam and Jones, 2018). Cyber systems create benefits, but they also introduce 'risk' (Kuhn et al., 2021b), which involves a state of uncertainty where some of the possibilities involve a loss, injury, catastrophe, or other undesirable outcome (Hubbard, 2020). 'Cyber risk' is the *"probability of a threat agent exploiting a vulnerability to cause harm to a computer, network, system, or utility, resulting in financial losses, disruption or damage to the reputation of an organization"* (Habash et al., 2013).

This thesis serves as a window into practice, illustrating the trends and fundamental concepts that characterise cyber risk in the maritime domain. Outputs 1-2 offer an in-depth look at cybersecurity and disruptive technologies in ports (Kuhn et al., 2021b) and vessels (Kipkech et al., 2022), and the space in-between. In this sense, one cannot ignore *"the three sides of the coin:"* ship, shore and their connections (International Maritime Organization, 2019). According to the IMO (2019), the harmonised collection, integration, exchange, presentation and analysis of marine information on board and ashore by electronic means is referred to as 'e-Navigation'.

Since the commercialisation of the internet in the 1990s, ships and ports have become smarter and their ICT systems more sophisticated. Digitisation, automation, information networks and integrated systems make vessels more connected than ever and are growing factors in shipping that make cybersecurity increasingly relevant. With such interconnected operations, a breach (deliberate or accidental) within one company in a supply chain can have serious knock-on effects for the other suppliers or organisations they work with (Grasso Macola, 2020). These inter-dependencies introduce new cyber threats to vessels that extend along the global supply chain, resulting in cascading risks (Tanczer et al., 2018) with catastrophic consequences. A single cyber attack on an ICT system can lead to crippling damage and network disruption (Cyberhedge, 2020), given that international shipping is a $183.3 billion industry (Tam and Jones, 2018) that facilitates around 90 percent of world trade (International Chamber of Shipping, 2020).

Cyber risk is a growing concern for all maritime actors, where there is a need for better training, specifically that which builds the decision-making capacity of senior executives. Understanding maritime cyber risk is a challenge as it is complex, evolving, and asymmetrical (De Smidt and Botzen, 2018); larger attack surfaces and greater uncertainty makes it hard to assess risk and formulate response. This is evidenced in Output 3 (Kuhn et al., 2020b) which informs on the current cyber threat landscape by examining challenges to adopt cyber insurance, a growing form of cyber risk management in the maritime sector. Accelerated digitisation, a result of COVID-19 (Kuhn et al., 2021b), is associated with increased cyber risk and that means less time for organisations to prepare response. While cyber incidents are inevitable, and risk cannot be eliminated, it must be managed. The varied nature of cyber threats means there is no single approach to address all resulting risks. The rate of technology change and the steady flow of serious vulnerabilities in operating systems, software libraries and applications mean that any strategy must be regularly reviewed. Organisations must consider risks and take stock of their capabilities to gauge their cyber readiness.

2.2 Game-based Learning for Enhancing Decision-making

This research takes inspiration from games and strategy exercises, which have evolved into a range of useful tools for military planning (Smith, 2010), disaster management (Walker, 1995), emergency preparedness (Johnson, 2008), safety (Smith et al., 2019) and national resilience (Gomez and Whyte, 2022). Planning for business risk mitigation arising out of cyber attacks could benefit from instincts and insights drawn from the decision-making process of participants, including risk perception and risk ownership.

Many simulations include scenarios, where a segment of the game is played and then participants are asked to reflect on game-play to draw behavioural insights or learning material is presented. The scenario may be fictional (Atlantic Council, 2019) or may simulate an organisation's structure and operations (Jalali et al., 2019). Previous research (Haggman, 2019) acknowledges the value of cyber attack scenarios for preparing analytical cybersecurity skills. Stretching the plausibility of the scenarios (including escalations of cyber-related risks) could be a useful dimension to articulate various challenges around mitigating risks from cyber attacks including stakeholder management, ownership, uncertainty and complexity. There is a trade-off to be had in scenarios that could be realistic on the one hand, and if pushed to be more *ahead of the times*, could serve to prepare for uncharted territory.

Games are a way to engage decision-makers that allow ecological validity to be controlled (if desired) to a high degree, including but not limited to degrees of uncertainty that participants might find in a reality. Although participants know the game is unreal, the designers must ensure the scenario is close enough to reality so that participants behave as they would in a real-life situation that the exercise emulates. Decision-makers are often confronted with cybersecurity challenges, which they may not fully comprehend but nonetheless need to address. Preparation through cybersecurity games is an invaluable tool to better prepare strategy and response to cyber incidents. Games offer capacity building to decision-makers through a controlled environment, often with hypothetical scenarios which invoke discussion, while decision-making skills are put to the test.

This research comes together at a time when cybersecurity games are high in demand. As such, the researcher is not alone in thinking about scenario-driven exercises to address cybersecurity. Other research (Frey et al., 2017) has developed games to explore security decisions in cyber-physical systems. International organisations and governments have also developed games, including NATO table-top exercises at the political strategic level (Lété and Pernik, 2017). Firms that sell cybersecurity as a product have developed cyber games, such as the Kaspersky Interactive Protection Simulation (KIPS) (Kaspersky, 2019). The game-based learning market has continued to grow since 2012 (Ogee et al., 2015), with revenues expected to reach over $24 billion by 2024 (Adkins, 2019). Yet, despite the investment being put into developing such exercises, their effectiveness for assessing decision-making and capacity building remains unclear. While previous work examines games for technical skills (Tioh et al., 2017), no work has looked at cybersecurity decision-making. This research assesses the effectiveness of games for cybersecurity decision-making and develops two original exercises to assess cybersecurity decision-making.

In the development of these exercises, this thesis builds on an extant literature base. The OCTAVE Allegro risk management method (Caralli et al., 2007) includes threat scenario identification, to support examination of threats to specific known assets. Threat scenarios may then expand the risk identification process across dimensions to include threats outside of the organisation's control, such as 'interdependency risks.' Such interdependent risks could be captured using a risk taxonomy and by connecting other roles in the organisation and the wider ecosystem, with a view to coordinating response and clarifying the role of cybersecurity in addressing risks. Other work (Rhee et al., 2012) explores whether top-level managers exhibit an optimistic bias toward their perception of the security risks which relate to their organisation. Rhee et al. (2012) found an appreciation for the interdependence between organisations, where we explore the relationship between such interdependence to state level, and the types of risk which may prompt risk response activities.

Other research (Shreeve et al., 2020) studies the decision-making of participants in a tabletop cyber-physical game. Shreeve et al. (2020) identify four structural patterns and two reasoning strategies to risk decision-making (risk-first and opportunity-first). They found their participants were driven less by risk-first approaches which identify an optimal response, and more by the responses that a team is capable of enacting within its existing capabilities and how successful those would be. This thesis explores the perceived role of different risk classes and actors in achieving acceptable security outcomes to emerging organisational risks.

The KIPS (Kaspersky Inc., 2021) is a commercial service targeted at increasing awareness of cyber-related risks at higher levels of management (specifically managers of business systems and IT). The offering is driven by a view that top-level managers in organisations differ in their perspective on cybersecurity risks. Scenario variations focus on training about identified threats to specific sectors, with a focus on how IT security can be managed in a way that does not hamper production facilities. Likewise, this research looks to elicit perspectives on related threats and challenges in coordinating an appropriate strategic response to cyber-related risks across cooperating stakeholders.

While this thesis is focused on the effective assessment of decision-making through simulation exercises, capacity building through *"experiential learning"* is another outcome (Smith and Elliott, 2007). Game-based learning uses an interactive format as a foundation for learning, where training content is woven into it (Growth Engineering, 2020). Such games are proven to boost engagement levels and increase knowledge retention (Chittaro and Buttussi, 2015). Within the context of cybersecurity, such simulations can be used effectively for learning (Jalali et al., 2019). Jalali et al. (2019) highlight the ability for capacity building exercises to offer benefits to decision-makers that come with minimal risk when they state *"the simulation environment provides a context in which to implement various strategies in any number of repetitions without fear of real consequences"*. Yet, to demonstrate effective teaching through games, participants would need to repeat the exercises over time to show improvement.

2.3 Enhancing Maritime Cybersecurity Decision-making

In risk management, the success of a decision is subjective in that it is dependent on how risks are understood (Hubbard, 2020), prioritised (Horne, 2017), managed and learned from. Most risk assessment methods rely on subjective inputs by human experts who make surprisingly consistent errors in judgement about uncertainty and risk (Hubbard, 2020). While this thesis considers that decision-making skills for risk management are consistent across different sectors, good decision-making becomes more challenging in sectors with greater uncertainly and greater risk. As such, good decision-making is more challenging in the context of cyber as it is complex, evolving, and asymmetrical (De Smidt and Botzen, 2018); greater uncertainty makes it hard to assess risk (Kuhn et al., 2021a). Decision-making is also more challenging in the maritime domain, where there are many stakeholders at risk (Lam and Su, 2015). When cyber and maritime are combined, decision-making becomes especially challenging due to accumulated risk (Kuhn et al., 2020b), where many developments including Internet of Things (IoT) have led to increased connectedness, where maritime cyber risks with a high degree of uncertainty (Sanchez-Rodrigues et al., 2010) are cascaded (Tanczer et al., 2018) amongst many stakeholders. Horne (2017) adds that since all organisations are different, effective decision-making differs according to the organisation, where *"each board needs to set its own direction and tone for cyber security"*.

Consequently, it is a challenge to objectively judge a decision as good. Moreover, *"entirely ineffectual but popular subjective scoring methods"* fail to consider the problems with subjective risks and introduce errors of their own to make decisions worse (Hubbard, 2020). Hubbard (2020) suggests that large, important decisions are best approached in another way. As such, this thesis does not go as far as to tell participants whether they make effective decisions, since it considers they are the experts in the room. Rather, it aims to 'hold a mirror' up to them by assessing them on competences that are key to the process of effective decision-making (as opposed to assessing the decision itself).

Key cybersecurity decision-making competences include (1) effective risk assessment by means of correctly perceiving incident severity to indicate proportionality of response; (2) correctly identifying risks to indicate understanding of wider business risks associated with cyber incidents; and (3) calibrated tendencies around risk prioritisation and decision-making in a group to form a strong security culture.

Firstly, a key decision-making competence includes effective risk assessment. Organisational leadership face all kinds of risks, many of which are distinct from the risks those in other roles must consider to reach informed decisions. Executive decision-making involves complex interactions between leadership teams, around *'episodic'* decisions and strategic issues (Nordberg and Booth, 2018). Senior leaders may receive new information from sources including news articles and peers, and delegate the evaluation of tools and technologies to security managers (Moore et al., 2015). To understand how risk is assessed, this thesis examines 'risk perception' which concerns potential impact, be it positive or negative, and the estimated likelihood of occurrence (Rogers, 1984). Risk perception is relevant for organisational leadership because it influences their decision-making (Massie, 2015). Understanding risk perception and its challenges allows for insights into strategic decision-making around cybersecurity.

To assess risk perception, this thesis assesses participants' ability to accurately perceive incident severity. This includes comparing perceived incident severity against actual incident severity (of escalating scenarios) to indicate the proportionality of their response. Errors in judgement by decision-makers, often due to incorrect risk perception, lead to a disproportionate response, which can cause mistakes in safety, resource allocation or incident escalation. In other words, gaps in perception of risk indicate gaps in capabilities to act (Williams, 2008). Thus, good decision-making includes a response that is proportionate to the risk.

Secondly, to assess risk perception, this thesis also assesses participants' ability to perceive (and prioritise) wider business risks associated with cyber incidents. This indicates their ability to correctly identify risks, whereas risk identification is a key competence of effective decision-making. This addresses the need to consider institutional factors within (and among) organisations, and to acknowledge *"important shared risks and relationships"* which are often ignored in existing risk management models that promote the unnecessary isolation of risk analysts from each other (Hubbard, 2020).

Thirdly, decision-making tendencies are a key competence which are assessed by asking participants to respond to scenarios in terms of whether they favour direct intervention, visibility, responsibility and urgency. These results are calibrated to offer insights into the groups *"direction and tone"* (Horne, 2017) for cybersecurity, which is an advantage to working with experienced decision-makers. That is, while exercises played by individuals may aim at capacity building, exercises played by groups can also aim at communication and thus offer an internal qualitative measurement system. This is especially relevant when working with groups of participants that have a wide range of backgrounds, such as work experience and cybersecurity expertise. This impacts risk perception: *"Risk, after all, is a matter of perception and every society has not only a different perception of risk, but also a different threshold for risk"* (Williams, 2008). These key competences and tendencies, when calibrated, indicate characteristics of a collective risk perception, which offers insights into security culture.

It is acknowledged (Rogers, 1984) that, among other factors, perception rests on a foundation of experience. Those who have not responded to a previous cyber attack of similar nature have little reference, which is a contributing factor to poor performance. This is not to say that to assess risk correctly, an organisation must experience an attack. There can be testing or 'drills' of security-related continuity plans. However, since organisations must respond to cyber incidents we consider learning for crisis and developing preparedness through simulations.

Chapter 3

Methodology

As discussed in Chapter 1, this thesis develops knowledge and an understanding of cybersecurity risks and decision-making within maritime environments. The two fundamental components underpinning the seven outputs relate to developing (a) a theoretical and conceptual framework and (b) new empirical knowledge. In this context, Outputs 1-4 relate to the theoretical and contextual framework, with Outputs 5-7 presenting new empirical knowledge. Research was conducted in line with Coventry University ethical guidelines. Results were anonymised for replication.

3.1 Developing a Theoretical and Contextual Framework

To establish the theoretical and contextual basis for this thesis, the researcher carried out a integrative literature review in line with established methods (Snyder, 2019). There are other literature review methods such as systematic review (which has specific research objectives and aims at synthesising the collection of studies) and semi-systematic review (which uses broad research objectives and is considered suitable for research with a broader topic within diverse disciplines). However, integrative review is most appropriate for this thesis, which aims to combine different perspectives, e.g., cybersecurity, decision-making, maritime. An advantage to the integrative review is that it allows for creative data collection, whereby the purpose of the review is not to cover all articles on the topic but rather to combine perspectives with the aim to assess, critique, and synthesise the literature in a way that enables the creation of new theoretical frameworks and perspectives (Torraco, 2005). This is most often used when looking at business literature (Mazumdar et al., 2005) or security literature (Amigud et al., 2018) where there are challenges to access confidential data.

Literature analysis was used in Outputs 1-3 to examine cyber risk in the maritime domain, looking first at ports (Kuhn et al., 2021b) and then vessels (Kipkech et al., 2022) (Outputs 1-2). Output 3 (Kuhn et al., 2020b) includes a review of literature around cyber insurance, using both academic, policy and industry sources. This was done by reviewing online news sources, policy documents and academic articles on the aforementioned topics. While the search was not systematic, it was done with the intent to bring together diverse sources to develop a narrative that reflects the complexity of the maritime cyber threat landscape. The purpose, to develop an understanding of maritime cyber risk, was realised by examining known cyber attacks, which provide context to ground the research.

Literature analysis on cybersecurity games is conducted in Output 4 (Hussain et al., 2020), the search also having included online news sources, policy, academic and industry documents. Data was collected through a online search which enabled the review of a greater number of games than what one-to-one interviews would have enabled. A data-set was compiled by reviewing related work, including a survey conducted by the European Union Agency for Network and Information Security (ENISA) which examined 200 cyber exercises that were executed between 2002 and 2015 (Ogee et al., 2015). Desk-based research was carried out to identify additional games executed between 2016 and 2019. After grouping multiple editions of the same game, this data-set contained 67 distinct cybersecurity games. Some games did not provide the information necessary for further data analysis. To improve the quality and reliability of the results, this list was further reduced to 46 games for data analysis. Then, a qualitative approach was used to investigate this data-set by reading through available information on the games, such as game highlights, presentations and after action reports.

The critical review and analysis of 46 cybersecurity games was based on four main areas of typical cybersecurity game format (Ouzounis et al., 2009), which includes: Game objectives, scenario injects, observation methods and evaluation methods- from which themes emerged.

Game Objectives

Game objectives were collated in a text file, which was fed into NVivo qualitative data analysis software for word frequency analysis. The word grouping was matched ‘with synonyms’. This algorithm matches words such as ‘building’, when it appears as ‘build’, ‘building’, ‘established’ or ‘making’. The analysis returned 50 most frequent words from which five themes emerged, as shown in Table 2.

Table 2: *Themes emerged from analysing game objectives of 46 cybersecurity games*

Capacity-building	skills, training, awareness, practice
Decision-making	critical
Engagement	cooperation, information sharing, communication, coordination
Incident management	incident response, risk management
Testing	plans, procedures, processes, identify, preparedness, improve

Scenario Injects

During game-play, information from a wide range of sources is provided to participants in the form of a scenario inject. This can include supporting cybersecurity evidence such as technical advisory, media items, non-confidential government or agency reports, confidential intelligence briefing, industry analysis and academic research. Scenario injects can have certain characteristics such as time pressure, escalation, reputation and resource allocation, which challenges decision-making, and are shown in Figure 1.

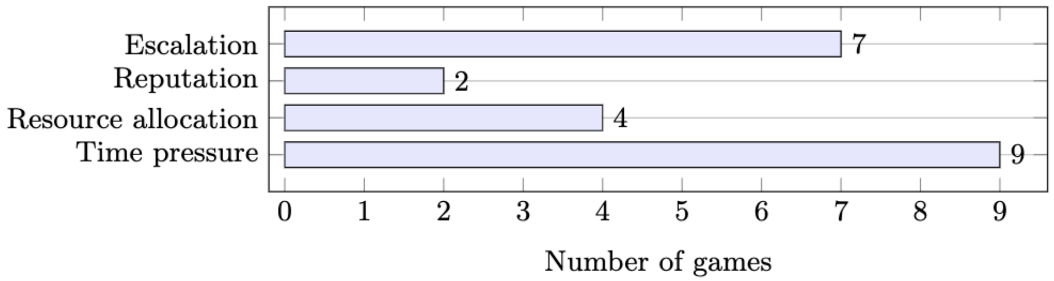


Figure 1: *Frequency of characteristics of scenario injects in 46 cybersecurity games*

Observation Methods

Observation methods are used for data collection in the form of computer-based observation, discussion, human observer, presentation, questionnaire and written submission. These are shown in Figure 2.

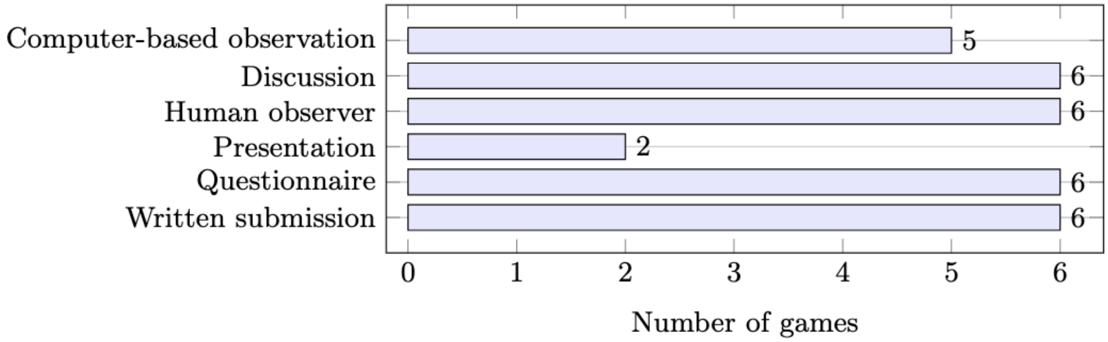


Figure 2: *Frequency of observation methods in 46 cybersecurity games*

Evaluation Methods

Evaluation methods are used to gauge effectiveness of games in the form of challenge solving, computer-based evaluation, expert judgement and participant self-reflection. These are shown in Figure 3.

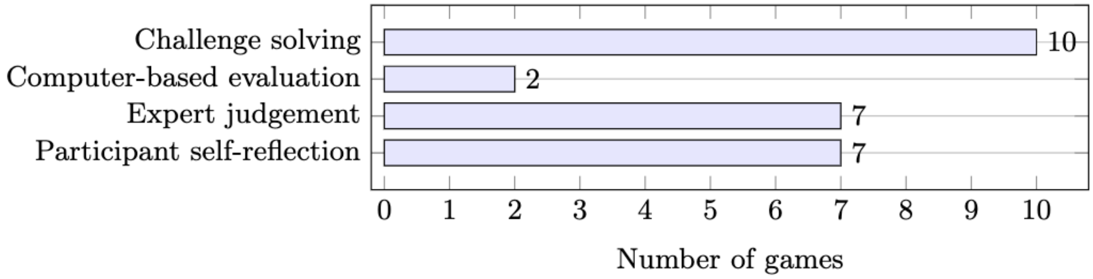


Figure 3: *Frequency of evaluation methods in 46 cybersecurity games*

From the above analysis of the 46 cybersecurity games, a criteria to assess decision-making skills in cybersecurity games is established, shown in Figure 4. The qualitative analysis of the data-set identified (1) five key themes of the game objectives, (2) four characteristics of scenario injects, (3) six observation methods, and (4) four evaluation methods. The criteria is composed of these elements. The 'lessons learnt' can feed into 'game design' for next editions to potentially improve the game. These two groups were not included in the criteria due to the fact that they exist outside of game-play. The components of this criteria provide insight into what makes an effective cybersecurity decision-making exercise. The purpose of this criteria is to inform the construction of a new such exercises for cybersecurity decision-making. This provides the contextual basis to develop simulation exercises.

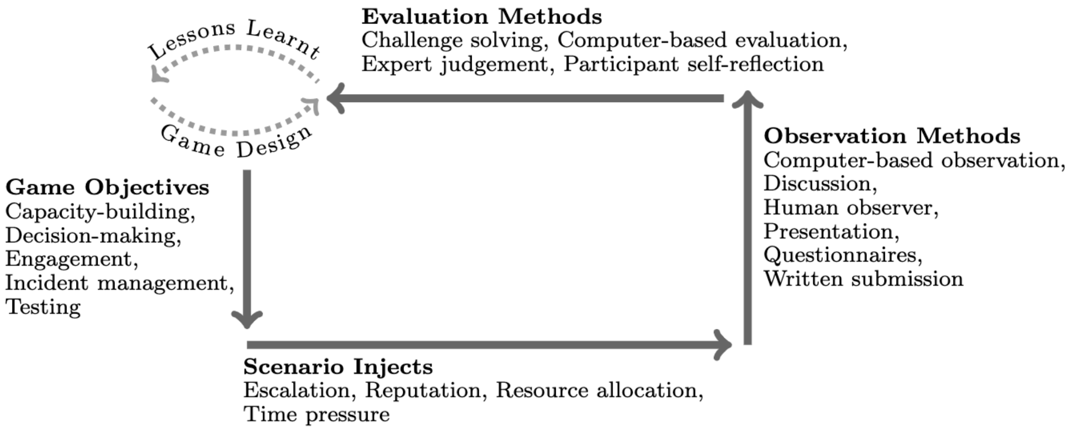


Figure 4: *Criteria to assess cybersecurity games for decision-making*

3.2 Developing New Empirical Knowledge

This section relates to Research Objective Three (Section 1.3), which includes developing, testing and applying scenario-driven exercises for executive decision-makers to understand cybersecurity risks and decision-making processes. This thesis develops two distinct exercises, where Exercise 1 (The Maritime Cybersecurity Game) is presented in Output 5 (Kuhn et al., 2020a) and in Output 6 (Kuhn et al., 2021a) and Exercise 2 (Scenario-Based Capacity Building Exercise) is presented in Output 7 (Parkin et al., 2021). The reason for developing two exercises is an identified opportunity to improve upon the first. After conducting Exercise 1, the researcher felt the study could be improved upon by assessing not only cyber risk perception and ownership, but the perception of wider business risks and so an improved version was developed.

While this research includes perspectives from maritime security, challenges associated with recruiting decision-makers (Section 1.5.2) led to the approach of different sectors.

While each sector (including maritime) is unique, all include cyber elements and as such are appropriate to conduct an exercise about enhancing decision-making about cyber risk. Consequently, participants were chosen based on our ability to access them via organisations to which they were affiliated. Exercise 1 participants included professionals attending a cyber course affiliated to NATO. Exercise 2 participants included Chief Information Officers (CIOs) and IT managers affiliated to a national science academy in Europe. It was key to have input from decision-makers at the senior executive level. To address this, and while the exercises included individuals from various organisations and sectors, all participants were selected on the basis that they had some responsibility for cybersecurity and/or organisational decision-making in their roles, as stated in the Participant Information Sheets (Appendix C). We can draw insights from data provided by individuals, such as work experience and technical expertise, to learn about the group and its affiliation- such as NATO members states which were represented in the course.

These exercises can be held remote or in person, and typically run half a day. The number of participants is ideally from 10-25 per exercise to foster a group discussion where all can participate, but more can be accommodated if necessary. During the exercise, participants are exposed to a three systematically constructed scenarios (S1, S2, and S3) which describe events applicable to their level of decision-making. The scenarios are written to capture the cyber threat environment of the organisation and that of the sector in which it sits. These are written as a narrative around a hypothetical organisation.

Several factors contribute to exercise design, the most prominent of which are: the maritime sector, cybersecurity and decision-making skills. The text below discusses the extent to which each of these factor influences the design of Exercise 1 (3.2.1) and Exercise 2 (3.2.2), as well as the probable impact on participants.

3.2.1 Exercise 1

Background to Exercise

Exercise 1 was conducted from March 9-13, 2020, at the “Terrorist use of Cyberspace Course” at The Centre of Excellence Defence Against Terrorism (COE-DAT) in Ankara, Turkey. There were 68 exercise participants. As the exercise was designed for 10-25 participants, the 68 participants were divided into four groups. This was done randomly by counting off 1-4 down an alphabetical name-list of course attendees.

Pre-exercise Questionnaire

Prior to the exercise, each participant was asked to complete the pre-exercise questions (Appendix D) about their work experience and cybersecurity expertise. The purpose of collecting this data was to have background information on participants from which to interpret the exercise results.

Development of Scenarios

The maritime sector is a key factor influencing Exercise 1 design. During the exercise, participants assume the role of “Cyber Incident Lead for the Maritime Response Unit of the National Security Council.” As such, they advise the head of government and private sector on cyber incident response, with specific regard to a fictional state-run container shipping company, Arden Ocean Shipping (AOS). In this context, participants are presented with scenarios designed around an escalating maritime cyber incident, seen in Table 3 (page 37). The scenarios escalate according to sector-specific impact levels (BIMCO, 2018), outlined in Table 4 (page 38). The benefit of playing through each scenario is exposure to incidents with varying degrees of impact (low, moderate, high). As participants rated incident severity according to these levels, they learned how to use sector-specific risk assessment tools for maritime; the probable impact being the establishment of the potentiality of game-based

Table 3: *Exercise 1 scenarios range over cyber incidents in the maritime domain and escalate according to the BIMCO impact levels detailed in Table 4*

Scenario
1. Unicorn of the Sea (Low)
AOS opens an arctic shipping route along Canada as opposed to Russia. The new AOS ice-breakers can access ports previously isolated to trade. This is a sore point for the Canadian Inuit community, as the route crosses waters inhabited by narwhals. The Inuit have spoken out against AOS, claiming ships will disrupt narwhals and may push them to extinction. This issue gains international attention. AOS is reacting to a media storm- many posts originating from Russia. The shipping line opens with *AOS Lunchbox* departing from the Port of Iqaluit. But the ship has not departed, as the port container terminal (PCT) system that controls cranes that load cargo on the ship has been down for two hours. When they try to access the system, dockworkers are redirected to the World-Wide Fund for Nature webpage with facts about the narwhal. Dockworkers cannot load the ship, and must work overtime until this is solved.
2. Parasite (Moderate)
AOS Peru reports Peruvian police found cocaine in the hull of *AOS Dina* embarking from Peru to Spain when they followed divers in the port, who planted it in a submerged ship compartment. However, when the ship sails the compartment where the drugs were hidden is not submerged. The criminals have manipulated the ship OT system which controls ballast, to lower the ship in the water to submerge the compartment, then raise her up- and repeat the process in the port of entry. This is hazardous to crew and cargo, as ballast grounds a ship. The cocaine was confiscated and the divers arrested. Police alerted Spanish authorities for suspicious activity when the ship arrives. However, this group can enter, undetected, into the control systems of at least one AOS liner. Fines associated with transporting illegal substances are large in countries where AOS has a presence, and ships may be arrested in ports of entry.
3. Sitting Duck (High)
AOS Jasmine, a semi-autonomous commercial liner, is stranded in the Persian Gulf. Ground control in the UAE cannot turn on the propeller. The area is known for piracy, but no one has boarded the liner. Communication is being interfered with remotely, stranding the ship across a busy traffic lane. An Algerian oil tanker diverts from course to avoid a collision with the liner, in turn hitting a fishing boat, killing nine. Responding to an SOS in national waters, Iranian military vessels search for survivors and redirect traffic. They also search nearby vessels, as they suspect one may be using a signal jamming device to remotely interfere with liner communication. Ship inspection grows more difficult as a traffic bottlenecks. The CEO of AOS receives an email from an unknown sender which demands the payment of $5 million to a bitcoin account, in exchange for the control of *AOS Jasmine*.

Table 4: *BIMCO Impact Levels defined and practical application*

BIMCO Impact Levels (Scenario)
Limited adverse effect (Low): Degradation in ship operation to an extent or duration the organisation can perform its primary functions, but effectiveness is clearly reduced. Loss of Confidentiality Integrity Availability (CIA) has a limited adverse effect on company and ship, organisational assets or individuals. Minor damage to assets, financial loss and harm to individuals.
Substantial adverse effect (Moderate): Significant degradation in ship operation to an extent and duration the organisation can perform its primary functions, but effectiveness is significantly reduced. Loss of CIA has a substantial adverse effect on company, ship, assets or individuals. Significant- damage to organisation assets, financial loss, and harm to individuals (not life-threatening).
Severe adverse effect (High): Severe degradation or loss of ship operation to an extent and duration the organisation cannot perform at least one primary function. Loss of CIA has a catastrophic adverse effect on company and ship operations, assets, environment or individuals. Major- damage to environment, assets, financial loss and harm to individuals (life-threatening).

Source: BIMCO (BIMCO, 2018).

learning for raising awareness of cyber risks at the senior executive level, Research Objective 4 (Section 1.3).

Cybersecurity was another factor influencing Exercise 1 design, as participants were not aware of the scenarios' escalation. This simulates reality, where decision-makers are often unaware of the severity of a cyber event underway. The probable impact is participants gain awareness of key challenges in cybersecurity decision-making, such as how to respond to an incident amidst uncertainty.

Decision-making skills is a key factor influencing Exercise 1 design. For each scenario, participants respond to four scenario inject cards, which represent situational changes to the scenario and require decision-making. These were taken from previous research (Hussain et al., 2020) that explores decision-making factors of such exercises. Each scenario includes a card which corresponds to the four injects listed and defined in Table 5. As participants are exposed to a range of injects that test decision-making skills, the probable impact is that their decision-making is not only tested, but improved.

Table 5: *Exercise 1 scenario injects and their operational definition*

Inject	**Definition**
Escalation	Increased severity of incident
Reputation	Shift in opinion of you or your company, causing loss or damage
Resource allocation	Available resources to be distributed between two or more things
Time pressure	Faster response is prompted

Four response attributes, based on those developed in the previous criteria (Hussain et al., 2020), are shown in Table 6. Scoring was done by ranking participant response on a scale (1-8) according to their reply to inject cards, whereby each reply has a preassigned weight. Each inject type is paired once with an attribute type, so for example an escalation card may be paired with a situation that teases out visibility, and the response is then added to the final visibility score, whereas each card weighs two points. This was done as an alternative to asking participants to simply rate their perceived response, to avoid confusion around application of terms. The game format is illustrated in Figure 5 (page 40).

Table 6: *Exercise 1 response attributes, expressed as options, and their operational definition*

Attribute	**Definition**
Direct intervention	Respond as involved actors, or ask intermediaries to intervene
Visibility	Respond clearly/openly or ambiguously/behind closed doors
Private sector ownership	Place responsibility on private or public sector
Urgency	Choose an immediate or delayed response

Operationalising the Scenarios

Exercise 1 was conducted in person at the COE-DAT training center in Ankara, Turkey. A game-based approach was used to construct the exercise, which was divided into three scenario rounds. Each scenario round was thirty minutes long in duration, to allow participants to read the scenario, ask for clarifications, and complete the scenario questions. Breaks of 15 minutes

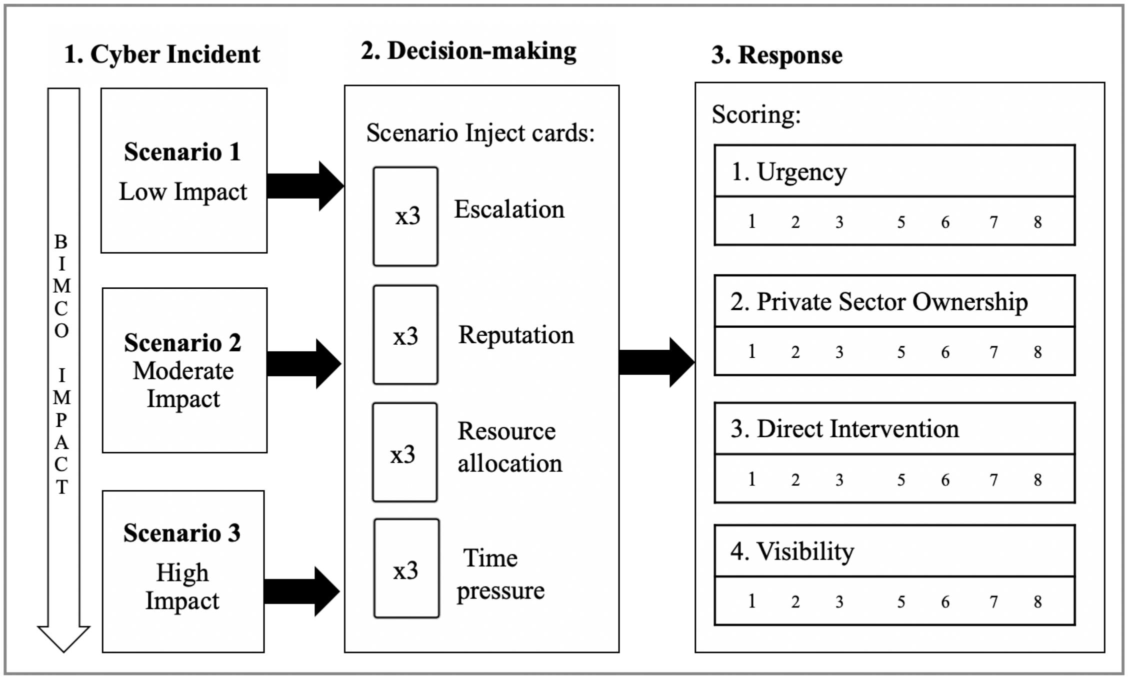


Figure 5: *Exercise 1 format includes three scenarios with maritime cyber incidents*

were taken between each scenario. For each scenario, the participant group is presented with a summary of the incident designed to evoke a response (as seen in Table 3 on page 37).

Scenario Questions

After reading each scenario summary, which includes three distinct scenarios that escalate according to incident severity ('impact level'- see Table 4 on page 38), the participants were asked (in their group) to response to inject cards which relate to the four injects in Table 5 (page 39), which relate to the response tendencies in Table 6 (page 39), using a group response sheet (Scenario Questions- Appendix E) that was handed out to the group, completed as a group, and collected by the researcher after the final scenario. At the end of the exercise, time was allowed for a group debrief and discussion.

3.2.2 Exercise 2

Background to Exercise

Exercise 2 (Parkin et al., 2021) participants included 19 CIOs and IT managers recruited through a national science academy in a European country. The background of the participants included a mix of public and private sector organisations. A few also held advisory roles in government, with responsibility for working closely with the private sector for cyber resilience. As the exercise was designed for groups of 10-25 participants, they were not mixed up or divided into groups.

Pre-exercise Questionnaire

Prior to the exercise, each participant was asked to complete the pre-exercise questions (Appendix D) about their work experience and cybersecurity expertise. This included asking them to rate perceived risks in their organisation, according to risk definitions provided which derive from the Cambridge Taxonomy of Business Risks (Cambridge Centre for Risk Studies, 2019). The purpose of collecting this data was to have background information on participants from which to interpret the exercise results.

Development of Scenarios

Exercise 2 design did not consider the maritime sector, as such the sector had no bearing on participants. Like Exercise 1, the scenarios (Table 7) escalate according to incident severity. These are written as a narrative around an organisation named "Company A". As the scenarios are not sector-specific, this escalation is captured by the six-category scale for cyber attack categorisation proposed by the NCSC (National Cyber Security Centre, 2018), seen in Table 8 (page 43). By designing and discussing scenarios according to this scale, scenarios elements were structured along a journey of increasing incident severity.

The scenario elements were designed to escalate across clear dimensions, shown in

Table 7: *Exercise 2 scenarios range over cyber incidents and escalate according to the scenario dimensions listed in Figure 6*

Scenario
Scenario 1
-The IT Team at Company A has reported a possible ransomware attack on their enterprise server, resulting in the encryption of the company's central data storage. -This has caused the company's accounts and finance, and human resources teams to have no access at all to their data. -The IT team have shared a communication from alleged hackers asking for a ransom of US$10,000 within three days from the receipt of the email. -The hacking group has threatened to post out stored credit card details of the company's customers on a public site, if the ransom is not paid. They have also threatened to cause further damage to the company. -The legal team, who have the remit to assure Company A's compliance with GDPR, have been asked to assess what liability is there to Company A. -The CEO has asked for an immediate investigation of the causes (including practices and behaviours) that may have led to this attack. Whether this attack has any other impact is also to be investigated.
Scenario 2
-The Estates Team at Company A has reported a malfunction with the digital building management system (BMS). The BMS is used to control the heating and ventilation of the entire HQ of Company A. This is a new system that has been operational only for the past year, and is critical to the company complying with national guidelines on managing the carbon footprint resulting from energy usage. The malfunction has caused the top floor of all the buildings in the HQ to be unsuitable for working, and staff located on these floors have had to work remotely for the past week. -The IT Team has confirmed that the new BMS is connected to the corporate IT network. They have confidently denied any link with the recent ransomware attack. They have asserted that the central data storage, which was the main target of the ransomware attack, has no link to the BMS even if both are connected to the corporate IT network. -The Estates Team have had the suppliers of the BMS investigate the malfunction. The BMS supplier has reported that they have not encountered such a malfunction before, and are not ruling out an intentional malicious attempt for which Company A has to take responsibility. The suppliers have argued their technology is in use all over the world for several years insisting their technology is reliable. -The above has raised tension between the IT and Estates Teams, as the possibility of this being linked to the recent ransomware attack has not gone away. The CEO has asked for the health and well-being of the staff affected in the relevant areas to be prioritised, along with a wider investigation.
Scenario 3
-The national media is reporting a nation-wide cyber attack on the country's infrastructure, targeting commercial and residential housing, and even infrastructure (including train stations and airport), around the country. The attack is affecting power supply to many of these buildings, directly affecting heating and ventilation systems, access control, and elevators and escalators. Stations and airports have been put on high alert, with many journeys disrupted due to cancellations. -A few days before the national incident (above), the national cyber security agency had approached Company A with a view to conducting a forensic examination across some of the computers, corporate network routers and PLCs interfacing the HQ building that was affected previously. The agency staff had confirmed that the impact of the attack on Company A had been a source of further disruption across buildings in other cities; exact details on the resulting impact are not known however. -More details on the national cyber attack have been released by the media, which point to a vulnerability in the digital BMS, supplied by the same supplier to Company A. The vulnerability affects the back-end cloud service provided by the supplier to allow for remote updating of the PLCs. Some of the reports have even pointed a finger to the attack that targeted Company A, calling it the source of the attack. The attack is being attributed to a neighbouring country who has long been an aggressor to its neighbours. While none of this information has been confirmed by the authorities, this has raised concerns amongst the top leadership of Company A. -The Board of Directors of Company A are now wanting more details from the IT and Estates Teams. Some of the Directors are wanting to issue a press release to assure the wider public.

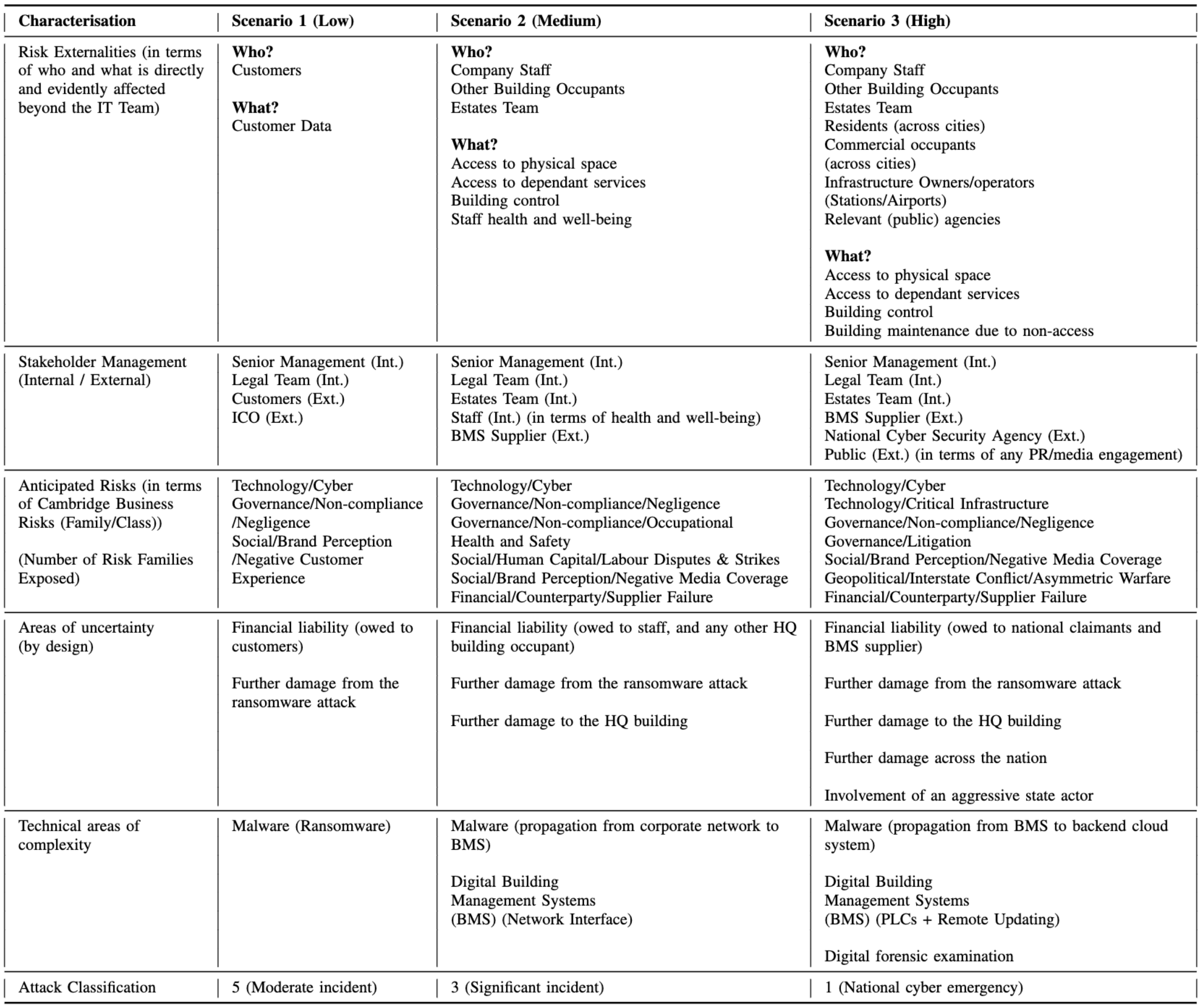
Table 8: *NCSC attack classification*

Attack classification
Category 1 (National cyber emergency): causes sustained disruption of essential services or affects national security, has severe economic/ social consequences, loss of life
Category 2 (Highly significant incident): has a serious impact on central government, essential services, a large proportion of the population, or the economy
Category 3 (Significant incident): has a serious impact on a large organisation or on wider/local government, or poses a considerable risk to central government/key services
Category 4 (Substantial incident): has serious impacts on a medium-sized organisation, or poses a considerable risk to a large organisation or wider / local government
Category 5 (Moderate incident): poses considerable risk to a small or medium-sized organisation, or preliminary indications of cyber activity against a large organisation or the government
Category 6 (Localised incident): poses considerable risk to an individual, or preliminary indications of cyber activity against a small or medium-sized organisation

Source: NCSC (National Cyber Security Centre, 2018)

Figure 6 (page 44), according to the risk level associated with the scenario and along which a participant may draw on judgement calls, as an executive involved in a management decision-making process and weighing up factors. These dimensions include: risk externalities; stakeholder management; anticipated risks; areas of uncertainty and technical complexity, and attack classification. For each scenario, a response from low to high is anticipated. In this sense, the exercise is as much about evaluating the scenario design approach as it is evaluating risk perceptions of participants.

Cybersecurity was a significant influencing factor in Exercise 2 design. Scenario content is informed by the researchers' knowledge of IT systems and processes which organisations are likely to have in place, and threats which can affect elements of a organisation's infrastructure. Moreover, known security incidents informed scenario design by signaling what may be possible. The scenarios draw on notable events such as the Norsk Hydro ransomware attack (Fiveash, 2019) (Scenario 1), the Blackbaud system compromise of 2020 which had potential ramifications for many organisations (Kelion, 2020) (Scenario 2), and the WannaCry (Morse, 2018) and NotPetya (Greenberg, 2018) attacks (Scenario 3). As



Characterisation	Scenario 1 (Low)	Scenario 2 (Medium)	Scenario 3 (High)
Risk Externalities (in terms of who and what is directly and evidently affected beyond the IT Team)	**Who?** Customers **What?** Customer Data	**Who?** Company Staff Other Building Occupants Estates Team **What?** Access to physical space Access to dependant services Building control Staff health and well-being	**Who?** Company Staff Other Building Occupants Estates Team Residents (across cities) Commercial occupants (across cities) Infrastructure Owners/operators (Stations/Airports) Relevant (public) agencies **What?** Access to physical space Access to dependant services Building control Building maintenance due to non-access
Stakeholder Management (Internal / External)	Senior Management (Int.) Legal Team (Int.) Customers (Ext.) ICO (Ext.)	Senior Management (Int.) Legal Team (Int.) Estates Team (Int.) Staff (Int.) (in terms of health and well-being) BMS Supplier (Ext.)	Senior Management (Int.) Legal Team (Int.) Estates Team (Int.) BMS Supplier (Ext.) National Cyber Security Agency (Ext.) Public (Ext.) (in terms of any PR/media engagement)
Anticipated Risks (in terms of Cambridge Business Risks (Family/Class)) (Number of Risk Families Exposed)	Technology/Cyber Governance/Non-compliance /Negligence Social/Brand Perception /Negative Customer Experience	Technology/Cyber Governance/Non-compliance/Negligence Governance/Non-compliance/Occupational Health and Safety Social/Human Capital/Labour Disputes & Strikes Social/Brand Perception/Negative Media Coverage Financial/Counterparty/Supplier Failure	Technology/Cyber Technology/Critical Infrastructure Governance/Non-compliance/Negligence Governance/Litigation Social/Brand Perception/Negative Media Coverage Geopolitical/Interstate Conflict/Asymmetric Warfare Financial/Counterparty/Supplier Failure
Areas of uncertainty (by design)	Financial liability (owed to customers) Further damage from the ransomware attack	Financial liability (owed to staff, and any other HQ building occupant) Further damage from the ransomware attack Further damage to the HQ building	Financial liability (owed to national claimants and BMS supplier) Further damage from the ransomware attack Further damage to the HQ building Further damage across the nation Involvement of an aggressive state actor
Technical areas of complexity	Malware (Ransomware)	Malware (propagation from corporate network to BMS) Digital Building Management Systems (BMS) (Network Interface)	Malware (propagation from BMS to backend cloud system) Digital Building Management Systems (BMS) (PLCs + Remote Updating) Digital forensic examination
Attack Classification	5 (Moderate incident)	3 (Significant incident)	1 (National cyber emergency)

Figure 6: *Exercise 2 scenario dimensions which represent a mix of elements designed into each scenario*

such, it is probable the participants found the scenarios to be credible. Further, like Exercise 1, participants were not made aware of scenario escalation. However, as the scenarios escalate, the level of uncertainty and technical complexity grows. To note, the former is not the omission of detail, but the inclusion of factors in a scenario which a security executive is not expected to have immediate knowledge of. The probable impact is participants gain an improved awareness of key challenges in cybersecurity decision-making, such as how to respond amidst uncertainty and technical complexity. Finally, after each scenario, participants were asked to identify areas of complexity and uncertainty, offering insights into why they made the decisions they did.

Decision-making skills are an increasingly significant factor influencing Exercise 2 design. This exercise adopts the Cambridge Taxonomy of Business Risks (Cambridge Centre for Risk Studies, 2019), shown in Table 9, to gauge the participants' perception and assess their response to many organisational risks which could be posed by a cyber incident. The probable impact on participants is increased awareness of the wider risks associated with cyber incidents, and knowledge gained through the experience trying to prioritise these risks. Further, they are prompted to take decisions with increased stakeholders. As measure of the response to the design regarding stakeholders, participants were also asked to indicate the scope of responsibility for the incident on a scale from private sector to state-owned.

Table 9: *Exercise 2 scenarios are assessed for anticipated risks as per the Cambridge Taxonomy of Business Risks*

Business Risks	**Examples**
Financial	economic outlook and variables, market crisis, trading environments, business and competition;
Geopolitical	national security, corruption and crime, government business policy, change in government, political violence, and interstate conflict;
Environmental	extreme weather, geophysical, space, climate change, environmental degradation, natural resource deficiency and food security;
Social	socioeconomic trends, human capital, brand perception, sustainable living, health and disease;
Governance	non-compliance, litigation, strategic performance, management performance, business model deficiencies, pension management, products and services;
Technology	targeted cyber attacks, critical infrastructure collapse, direct and indirect industrial accidents and the inability to keep up with advances in technology.

Source: Cambridge Taxonomy of Business Risks (Cambridge Centre for Risk Studies, 2019)

Operationalising the Scenarios

Exercise 2 was conducted online via Zoom due to social distancing because of COVID-19. A game-based approach was used to construct the exercise, which was divided into three scenario rounds. Each of the three scenario rounds was 40 minutes long in duration, to allow participants to read the scenario, ask for clarifications, complete the scenario questions, and to allow for occasional breaks. For each scenario, the participant group is presented with a summary of the incident designed to evoke a response (as in Table 7 on page 42).

Scenario Questions

After reading each scenario summary, the participants rated the incident severity ('attack classification'- Table 8 on page 43), and then selected and ranked the business-related risks which they perceive as being present, using an individual online response sheet (Scenario Questions- Appendix E) that was contructed in Excel and stored on OneDrive. As this was conducted online, it was deemed by the researcher more effective to capture individual responses than coordinate group responses. At the end of the exercise, time was allowed for a group debrief and discussion.

In terms of risk ownership and the responsibility to mitigate risk, participants were also asked to position the split of responsibility between state and private sectors on a Likert scale – at either end of a 6-point scale were state responsibility (1) and private sector (5), with the mid-point representing equally-shared responsibility. In closing each scenario-specific round, participants were also asked to note any areas of uncertainty and particular technical complexity they felt were present in each scenario (these were free-text questions).

Systematic Content Analysis

Systematic content analysis is used to gain further participant insights in Exercise 2. The methodology so far aims to establish the ability of the exercise to effectively capture insights from decision-makers and to demonstrate the perception of a wide array of business risks and stakeholders in decision-making, and content analysis provides further insights into why various business risks are considered. This allows for the interpretation of results not only at face-value, but offers understanding as to why participants made the decisions they did during the exercise. That is, Exercise 2 captures not only decisions, but probes participants for insights onto their decision-making process. Content analysis is an appropriate method as it may be used to *"explore the human experience"* (Erlingsson and Brysiewicz, 2017). Here, decision-making (human experience) is studied through analysing textual data collected in a focus group (semi-structured interview data). The objective in qualitative content analysis is to systematically transform a large amount of text into a highly organised and concise summary of key results (Erlingsson and Brysiewicz, 2017). An effort is made to take qualitative data and to quantify it to some degree, by coding each item (dividing up text into meaning units) and then categorising items into themes.

Exercise 2 included a discussion at the end of each round, where participants were able to raise any points or clarifications about their thought process when responding to the scenario. From this process, empirical data was collected using the Scenario Questions (Appendix E). This includes reflections raised throughout the exercise on the topic of uncertainty (Q4) and technical complexity (Q5). This data, from which quoted comments also derive, is categorised and emerging themes offer insights which strengthen the researchers' ability to interpret exercise results.

3.3 Ethical Considerations

This research was conducted in line with good qualitative ethical practice. All required steps were taken to obtain ethical approval from the corresponding body within Coventry University. This includes ensuring participatory consent (Annex B), due governance of data collection (including storage, processing, sharing and deletion in compliance with GDPR), digital needs met through secure infrastructure, and following COVID-19 social distancing protocols. Participants were also provided with an information sheet (Appendix C) outlining the aim, background and rationale for the research, and why they were selected to take part.

The principles of the Menlo Report (Dittrich et al., 2012) for ethical research in ICT are also addressed. The question sets were devised and screened to ensure that they are of an appropriate nature and do not cause undue stress to participants. This includes question design that did not require sensitive business details to be revealed, and an environment which encouraged participation, while also recognising the busy schedules of participants and the time they contributed to the activity; for instance, data collection and questions were designed to facilitate short answers. Participation was voluntary, with participants provided a high-level executive summary of results and reflections. All steps were taken to ensure that information was held confidentially by the researcher, as anonymity within this research is essential. Moreover, anonymity is assured within the published works by not disclosing participant names, affiliations or places of work. The study also ensured no hindrance of fair representation of diversity (in terms of age, disability, race, gender, religion, sexual identity).

As the key findings of this thesis can be strengthened by further iterations of the exercises presented, the data and methodology needed to replicate the exercises were anonymised (in line with ethics) and made accessible to the research community in two ways. First, the data and methodology are elaborated upon in Chapter 3 (and its associated appendices) to the extent that other researchers could replicate the results. Second, two licensed data-sets are publicly available on The Pure Portal, where they are linked online to relevant publications: Data-set for Exercise 1 (Kuhn, 2022a); Data-set for Exercise 2 (Kuhn, 2022b).

Chapter 4

Results

The previous chapter presented the methodology underpinning the seven outputs, including a fundamental component that relates to developing new empirical knowledge (Section 3.2). This component incorporates two distinct exercises for executive decision-makers, where participants respond to an escalating cyber incident presented across three scenarios. This chapter builds on that by providing an analysis of the results of these exercises conducted across the research portfolio. In this way, the developed exercises are tested and applied, to fulfil Research Objective Three (Section 1.3). This chapter is structured in a way that for each exercise, the results gathered include analysed data collected from the pre-exercise questionnaire (Appendix D) and from the scenario questions (Appendix E). In doing so, this enables a greater understanding of cybersecurity risks and decision-making processes through insights which relate to (1) earlier participant experience and expertise; and (2) participant response to an escalating cyber incident.

4.1 Exercise 1 Results

Exercise 1, presented in Output 5 (Kuhn et al., 2020a) and Output 6 (Kuhn et al., 2021a), is designed to test and interpret response tendencies of a group to an escalating cyber incident. It does this by analysing background information on participants from which to interpret the exercise results, which include tendencies that characterise response according to incident severity. This offers insights into the decision-making process of a group at different levels of perceived cybersecurity risk.

4.1.1 Pre-exercise Questionnaire Results

To collect background information on participants from which to analyse exercise results, we sought to understand the breakdown of their work experience by sector. This is because the participants, recruited through NATO, were thought to have significant military/public sector experience and previous research (Carr, 2016) highlights this as a factor governing cybersecurity response tendencies (most notably in relation to private sector ownership).

Analysing the pre-exercise questionnaire results (Appendix F), Figure 7 shows the breakdown of the years participants spent in the public/military sector and Figure 8 shows the breakdown of the years participants spent in the private sector. To confirm, participants exhibited significant public/military sector experience (89 percent had at least five years) and varied private sector experience. It is interesting that while all participants reported their public/ military sector experience, over a fourth (28 percent) did not report their private sector experience. This may be due to the confidential nature of their work.

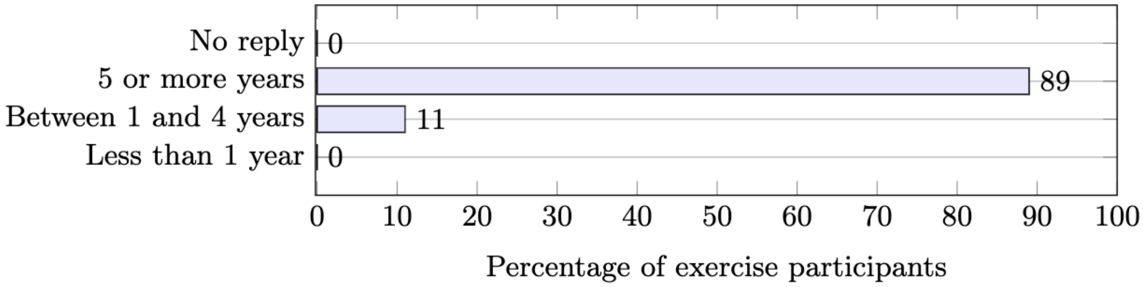


Figure 7: *Exercise 1 participants public/military sector experience*

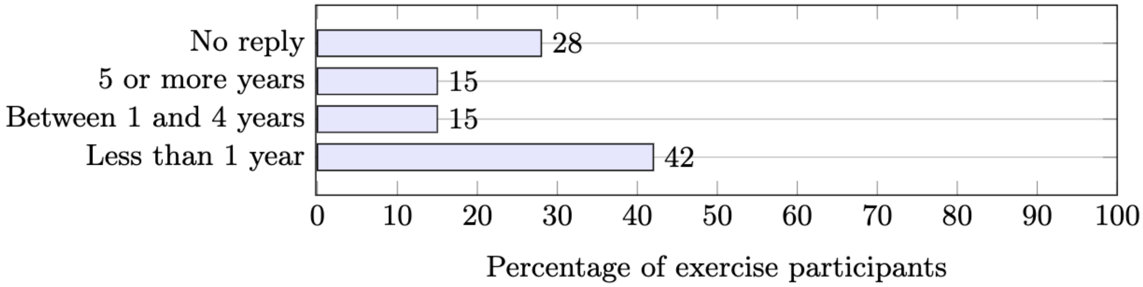


Figure 8: *Exercise 1 participants private sector experience*

To collect further background information on participants from which to analyse exercise results, we sought to understand the breakdown of participant cybersecurity expertise. This is because previous research (Tioh et al., 2017) and new guidance for improving cybersecurity in organisations (National Cyber Security Centre, 2019) highlights the importance of technical understanding of cybersecurity as a key factor governing response. As such, the pre-exercise questionnaire results also offered insights into participants cybersecurity expertise, shown in Figure 9. This includes how they ranked themselves in terms of their expertise in cybersecurity. The group exhibited varied expertise, with most participants rating themselves as either beginner or intermediate (83 percent). Less representation (17 percent) was exhibited from those who rated themselves either novice or expert, the two extremes on this spectrum. This may be because cybersecurity is a highly technical field, where people enter into executive roles with some experience and are unlikely to classify themselves as novice; however, they may acknowledge the complex and evolving nature of cyber, and hesitate to classify themselves as an expert.

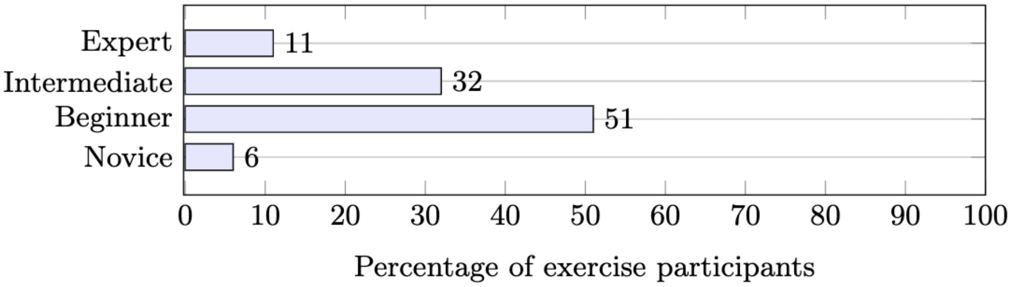
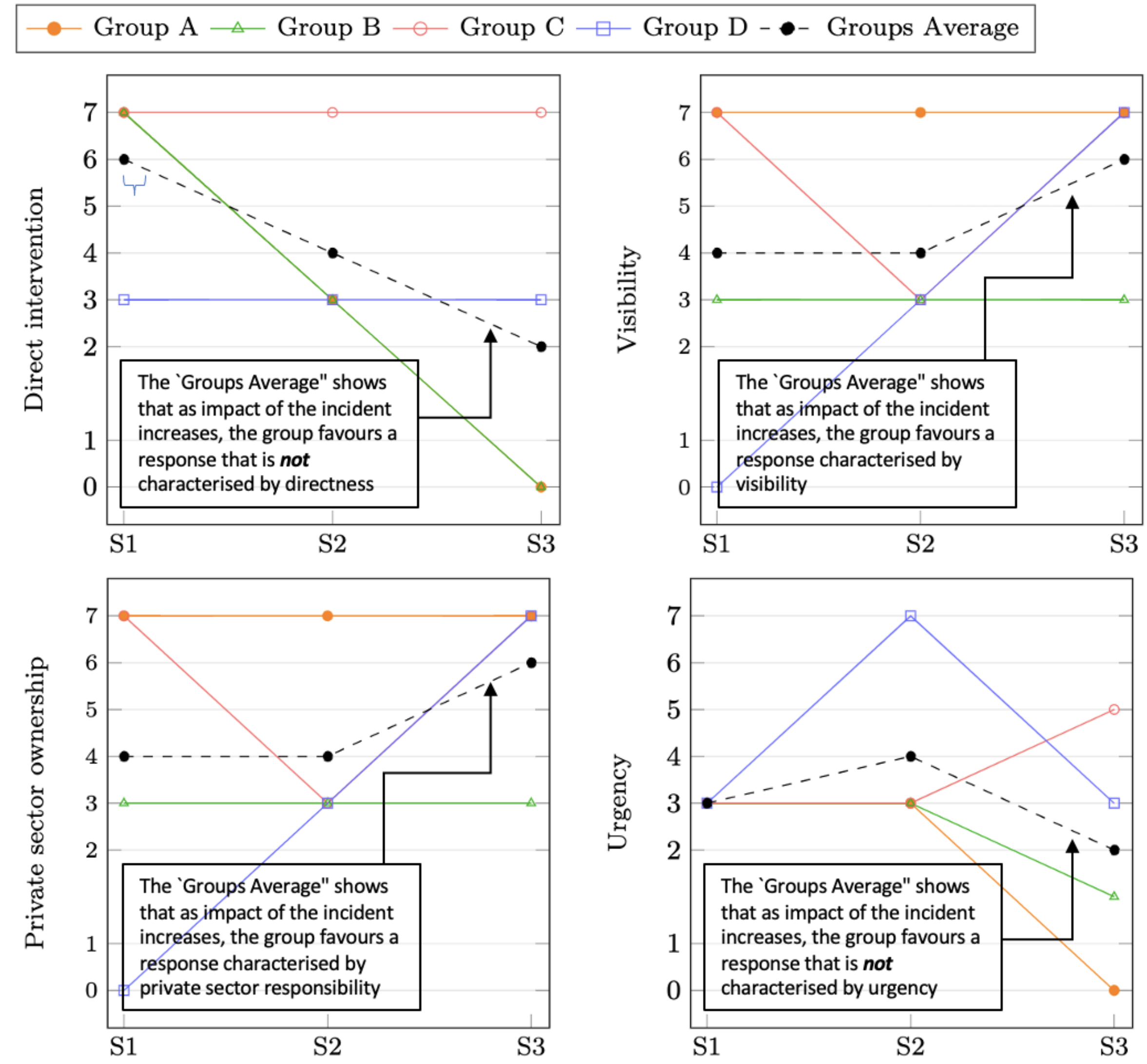


Figure 9: *Exercise 1 participants cybersecurity expertise*

4.1.2 Scenario Questions Results

Looking next at scenario questions results (Appendix G), Figure 10 shows participant response to the changing impact levels, which is interpreted through the participant data anaylsed. Accounting for significant work experience in the military/public sector, we may interpret the results to understand tendencies of the participant group and infer about cyber incident response behaviours of NATO military officers and equivalent civilians. This is important as it offers insights on tendencies which characterise the NATO security culture, from which emerges a collective risk perception.

The graphs in Figure 10 show ranked response tendencies to four key response attributes, for which the operational definition is provided in Table 6 on page 39. The trend lines ("Groups Average") suggest that as the impact of the incident increases, the group favours



The `Groups Average" shows that as impact of the incident increases, the group favours a response that is ***not*** characterised by directness

The `Groups Average" shows that as impact of the incident increases, the group favours a response characterised by visibility

The `Groups Average" shows that as impact of the incident increases, the group favours a response characterised by private sector responsibility

The `Groups Average" shows that as impact of the incident increases, the group favours a response that is ***not*** characterised by urgency

Figure 10: *Exercise 1 incident response ranking of scenarios (S1, S2, S3)*

a response that is characterised by (1) private sector responsibility and (2) visibility, but not by (3) urgency or (4) directness.

First, group urgency of response- which refers to whether the response is immediate or delayed- decreases as the impact of a cyber incident rises. This may reflect the idea that while small-scale cyber attacks may be the work of criminals, larger-scale attacks are more likely the work of organised or skilled actors, such as states, with increased resources to support a complex attack and a long-term outlook. In this sense, '*'Law enforcement and* *military authorities seeking to check malicious cyber activity face another fundamental challenge: the 'attribution problem' of identifying the author of a cyber attack or cyber exploitation"* (Goldsmith, 2013). While there may be pressure to name an adversary, the consequences of naming the wrong one early on often outweigh the cost of delaying response while information is gathered and verified. Indeed, the main hurdle is verification, which is difficult in the cyber realm due to attribution.

Second, as incident impact increased, the group favoured a response led by the private sector, as opposed to the government, although the response did include a combination of both. This is interesting finding, as we estimated there would be a tendency to favor government-led response because in many countries military is closely aligned to state. Further, the 2019 Global Cyber Risk Perception Survey (Marsh LLC and Microsoft, 2019) reports a *"strong appetite for government leadership and support"* to help combat cyber threats. However, the opposite is observed: as impact increased, group response favored the private sector. One explanation is that as a cyber incident escalates, the government becomes reluctant to claim mandates to oversee network security. Yet, it is often the case that the private sector is not inclined to accept responsibility or liability for national cybersecurity. This tendency is noted in previous work (Carr, 2016) concerning the challenges of public-private-partnerships. Another factor at play is that *"the private sector has their hands deep in cyberspace in a way very difficult for the government to match"* (Healey, 2017). Wide expansion of IT products and services makes it difficult for the government to keep up with the private sector, thus they rely on it. Consider that nearly 90 per cent of US critical infrastructure is in private hands (Weinstein, 2019). It is plausible this participant group, who comprise largely of military officers, are aware of this fact and thus rely on the private sector.

Third, group visibility of response- which refers to whether the response is clear/open or ambiguous/behind closed doors- increased along with incident impact. This may have to do with the fact that, while smaller incidents are easier to keep hidden or covert, large-scale cyber attacks are difficult to hide. Therefore, visibility reflects a greater need for assurance to those affected by and aware of the incident, such as the public or the international community.

Finally, as incident impact increased, group response was less direct- this refers to a response by the involved actors, as opposed to intermediaries who intervene on their behalf. This may be because as the impact of a cyber incident increases, so does its scale and complexity– to a point that a collective and multi-faceted response is required, especially in the context of NATO. This is evidenced in the case of Russian hacker group "Cozy Bear" (APT29) targeting COVID-19 vaccine researchers (North Atlantic Treaty Organization (NATO), 2020), where NATO was the first body to indirectly articulate information collected by various allies, including Canadian, UK, and US government institutions.

These results are important because they offer insights into risk perception, a major aspect in maritime cyber risk management that, while complex, is key to effective decision-making and cyber incident response (Williams, 2008).

4.2 Exercise 2 Results

Exercise 2, presented in Output 7 (Parkin et al., 2021), is designed to test and interpret risk perception and response to an escalating cyber incident. It does this by analysing background information on participants from which to interpret the exercise results, which include perceived incident severity ('attack classification') and perceived business-related risks (which were identified and ranked). Participants were also asked to position the split of responsibility between state and private sectors, and to note any areas of uncertainty and technical complexity in each scenario. This offers insights into the decision-making process of individuals at different levels of perceived cybersecurity risk.

4.2.1 Pre-exercise Questionnaire Results

To collect background information on participants from which to analyse exercise results, we sought to understand what business risks they perceived as top cybersecurity risks to organisations. This is because organisational leadership faces all kinds of risks, and understanding how these are perceived allows for insights into strategic and guiding decisions taken around cybersecurity and cyber incident response (Parkin et al., 2021). Looking first at pre-exercise questionnaire results (Appendix F), Figure 11 shows that all six risk categories were ranked by the participant group, although where they appeared in the ranking differed. As might be expected, where 'Technology' was ranked by participants, a 1st-place ranking appeared more here than for any other category, and relatively high up the list (no participants ranked it 5th or 6th). No participants ranked 'Environmental risks' in 1st place, but interestingly at least two or more participants ranked every other category as the most important risk to an organisation before seeing the scenarios. We can interpret these results to mean the group perceived a wide array of business risks associated with a cyber incident and this informed how they answered the scenario questions.

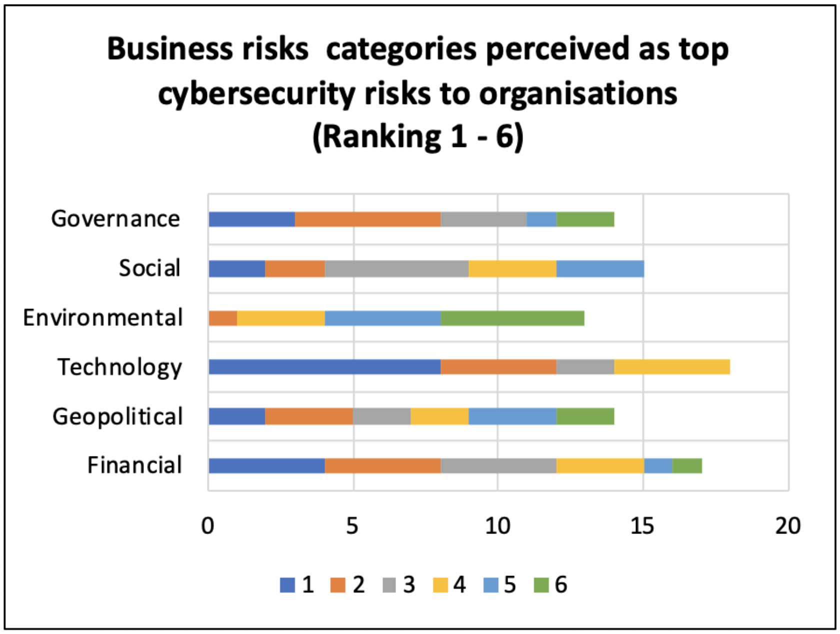


Figure 11: *Top perceived cybersecurity risk categories, from the pre-exercise survey (1 highest, 6 lowest). The x-axis indicates the total number of participants who have included each category in their ranking*

4.2.2 Scenario Questions Results

As risk perception influences decision-making, we wanted to see if participants could perceive rising incident severity in an escalating cyber incident. Looking at perceived incident severity, Figure 12 uses data from the scenario questions results (Appendix G) to show scenario attack categorisation, where participants noted a shift in the general severity of the scenarios as the complexity and severity increased (see Figure 6 on page 44). This was certainly the case from S2 to S3, if not S1 to S2. This is important because it indicates that the design of increasing severity through 'medium' may require attention to articulate an intermediate set of circumstances. The radar chart shows how the categorisation selection was spread across participants- even in the limited cohort, there was some convergence but not absolute agreement on how to categorise incidents. This means that the participant group perceived rising incident severity in the escalating cyber incident presented.

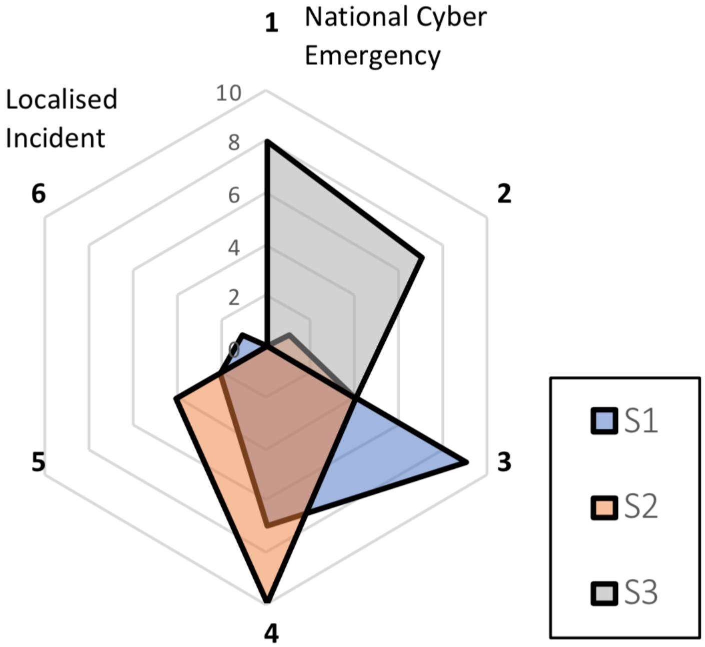


Figure 12: *Radar chart showing number of selections by participants of each attack category. Each vertex represents one of the six defined 'attack classification' categories, category 6 for a localised or emergent incident, and category 1 for a national cyber emergency*

As participants were able perceived a wide array of business risks in relation to a cyber incident (see Figure 11 on page 56) and they were also able to perceive increase severity of an escalating cyber incident (see Figure 12 on page 57), we were interested to see how their perception of anticipated business risks changes as the cyber incident escalates. This offers insights into how decision-makers manage complexity and what risks motivate their response. Figure 13 (page 59) shows the diversity of indicated risk categories increased as the scenarios became more complex, represented simply as the average number of risk categories selected by participants for each scenario (participants could select one or more). For S1 the average is 2.68; S2, 2.84, and; S3, 3.63. As the scenarios were designed to include 3, 4, and 5 risks (See "Anticipated Risks" in Figure 6 on page 44), the general trend of increased risks was captured by the group and, within expectations, S3 shows the greatest divergence of categories being selected (the 'complexity' of the risk landscape was seen by participants to have broadened). This is meaningful because it indicates that executive decision-makers can anticipate wider business risks as a cyber incident escalates. In terms of what risks motivate response, financial risk was seen as the 'top' risk for S1, Technology for S2, and Geopolitical for S3. No one risk category was completely ignored, though we may regard Environmental (for S1) and Geopolitical (S2) as having been categorised as non-critical risks. For each scenario, there were categories which were ranked differently by different participants (e.g., Financial in S1, Social and Technology in S2, and Social and Technology in S3). That is, a factor was seen as important, but opinions on *how* important it was differed, in some cases across the entire ranking scale. This is important as it suggests that while decision-makers may all be able to identify wider risks, the importance of each is perceived diversely, which means that conflicting priorities may undermine a coordinated response.

Given that private sector ownership increased with incident impact was an interesting finding in Exercise 1 (Figure 10), and previous research (Carr, 2016) highlights this as a factor governing cybersecurity response, we wanted to test this finding with another participant group who did not have significant military/public sector experience. To understand the responsibility mix in Exercise 2, participants were asked to indicate their perception of the

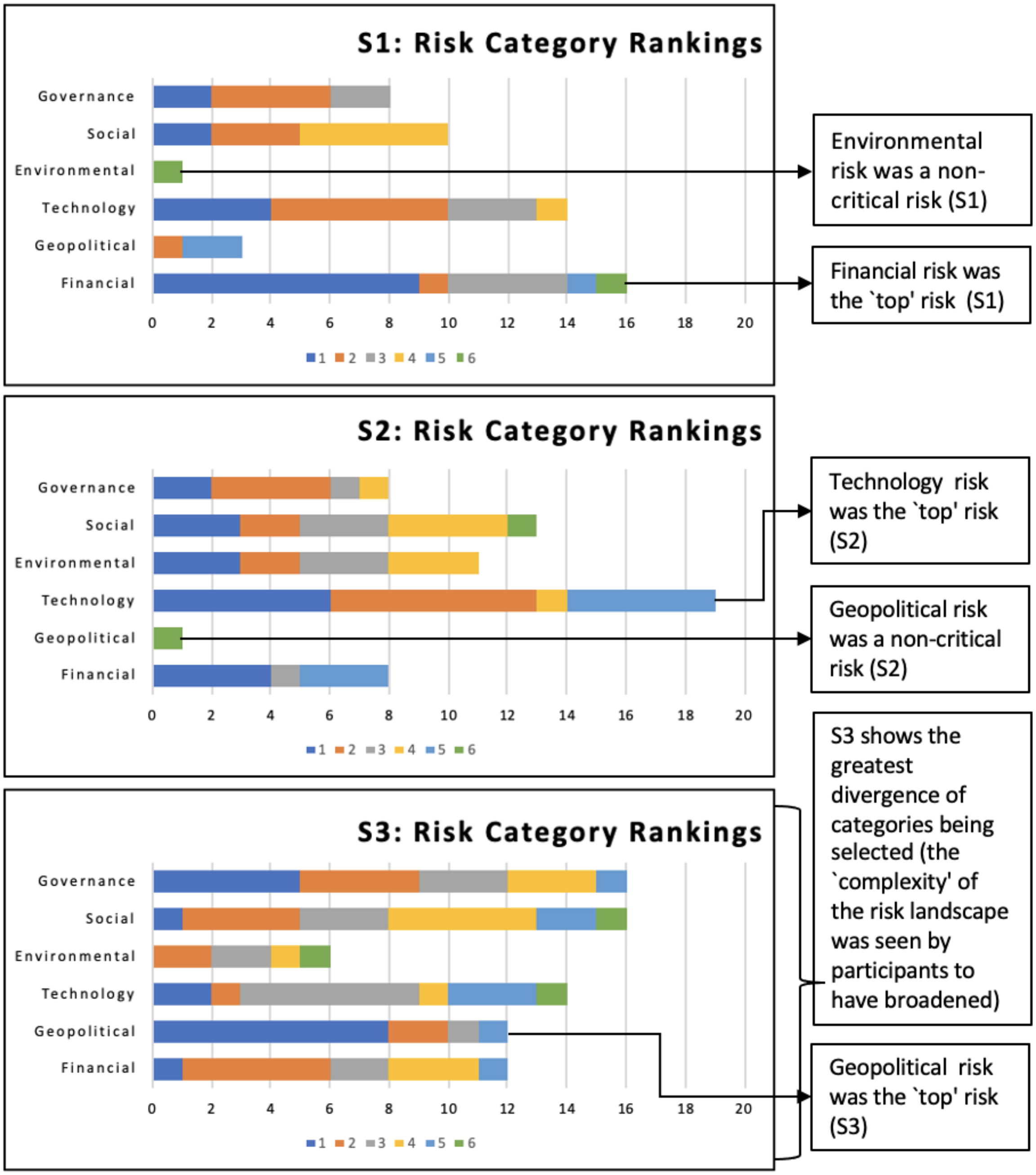


Figure 13: *Business risk category rankings by number of participants, for each of the three scenarios (1 highest, 6 lowest). The x-axis indicates the total number of participants who have included each category in their ranking*

private-public mix of responsibility for risks seen in each scenario (Figure 14), on a scale of 5 (private sector) to 1 (public/ state). Values around the centre of the scale indicate

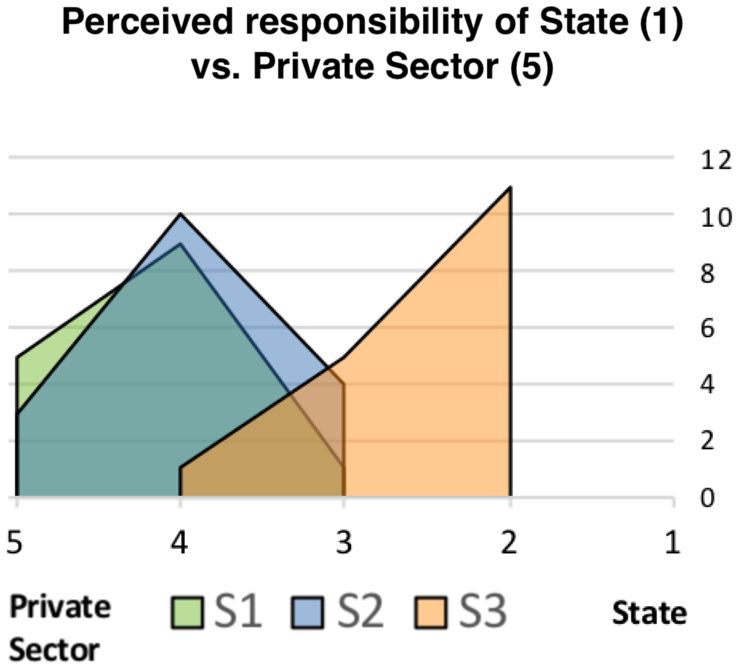


Figure 14: *Tally of participant perception of the responsibility of the organisation ('private sector') against that of the State in managing the risks in each scenario (S1–S3). The y-axis indicates number of participants who have selected each of the values 1 ('state') to 5 ('private Sector')*

shared responsibility. Figure 14 shows a transition akin to a 'wave' when stepping through the scenarios, marginal from S1 to S2, and pronounced from S2 to S3. It is interesting that the range for each scenario is within two steps on the scale – 5–3 for both S1 and S2, and 4–2 for S3, with a slight shift of perceived responsibility toward the State in S2 compared to S1. While no participants perceived any one scenario as being the sole responsibility of the State, the shift towards state responsibility is meaningful because it shows the opposite trend identified in Exercise 1. Collectively, the results suggest that while a group with military/public sector experience hold the private sector responsible to respond to severe cyber incidents (Exercise 1), those without significant military/public sector experience hold the State responsible (Exercise 2). This affirms previous research (Carr, 2016) that claims public–private partnership is a *"nebulous arrangement"* where no sector is inclined to accept responsibility or liability for national cybersecurity.

To be able to interpret the results above, or *why* participants responded the way they did to the scenarios, further empirical data was collected in the scenario questions results (Appendix G) with regards to uncertainty and technical complexity. The key results from content analysis, including themes, along with some of the related areas addressed in the discussion that followed each scenario, are summarised below.

For Scenario 1, participants observed that the scope and impact of ransomware attacks needed validation. Often there is a knee-jerk response to ransomware (regarding whether the ransom is paid, who is behind the attacks, and so on). The implication is organisations should consider more carefully what existing procedures could be invoked (in terms of backup and recovery options) and how to assess the veracity of the claims being made by perpetrators. Ransomware depicts uncertainty in terms of the actual danger it poses, and the need for validation. In response to Q4 (uncertainty), P8 captured this when they commented *"The full extent of the damage is not clear. It is uncertain whether there was a breach of internal security protocols and whether someone internal to the company is responsible, intentionally or not".* This is meaningful in that it affirms claims (Moore et al., 2015) that senior security managers may have a sense that the nature of uncertainty means not all risks can be mitigated. While the scenario was designed to carry a certain level of complexity, several participants expressed the need for more detail to better assess the scenario, with P13 commenting *"More information is needed regarding the segmentation of the networks and backups to draw any definitive conclusions"* in response to Q5 (technical complexity).

For Scenario 2, the nature of the customer-supplier relationship was a particular point of discussion. Regarding how much responsibility suppliers carry, this was expressed both in terms of: (1) What support they offer to investigate and recover from serious incidents, and; (2) How contractual terms with suppliers need to cover for liabilities that customers carry. In response to Q4 (uncertainty), participants explicitly challenged *"Who is responsible for the resolution of the problem?"* (P1), and *"What is most important to be established is where the actual liability is - with the supplier or with Company A?"* (P8). Nearly a third of the participants raised questions around the exact nature of responsibility carried by the supplier in response to such an incident. This is key as it affirms that participants also acknowledge that public–private partnership is a *"nebulous arrangement"* (Carr, 2016) even though they were later inclined to hold the State responsible. The nature of escalation in Scenario 2, which was posed by the introduction of the building management system (BMS), also raised the level of perceived complexity, as noted by a quarter of participants. In response to Q5 (complexity) comments ranged from the exact nature of the connection between the corporate network and the BMS, and the potentially unique vulnerabilities carried by such systems.

For Scenario 3, the participants highlighted the responsibility split between state and private sectors, within the context of a major incident. The role of national agencies and organisational responsibility to wider national stakeholders was also questioned. This was set in the context of different national policy frameworks and ecosystems. The participants' shift to holding the state responsible for the incident is clear from Figure 14 on page 60; governance and social risks were seen as of importance to most of the participants, but with varying levels of priority associated with it. The shift to State responsibility was summed up by two of the participants, who made this explicit: *"If there is a national threat, shouldn't the State support the investigation?"* (P7), and *"In any such situation, there is a need and necessary actions that the State must take with regard to the strategic objects of national security."* (P14). Interestingly, the participant responses to free-text questions support the trends captured in Figure 14. Senior security managers in some organisations may also be proactively briefed by the State about emerging threats (Moore et al., 2015). The range of complexities posed by this scenario were captured, where some of the key themes raised by the participants include the *"attribution to neighbouring states"*, sector-specific inter-dependencies, *"cascading effects"* from cyber attacks, a need for greater communication between agencies and private sector, and *"technology support for [public limited companies]."* This is meaningful as it shows participants saw that the importance of each risk is perceived diversely, and that conflicting priorities might undermine a coordinated response– to be countered by improved communication.

Chapter 5

Research Journey

This chapter presents a synopsis of the research outputs, listed in Appendix A, in the order they were undertaken by the researcher (see Table 1 on page 19). Each subsection summarises the output methodology and states the researcher's role alongside that of collaborators. It then reflects on the choices made at each point in the research journey and where more information or data gathering could have led to more proficient insights. While the scale of this research demands collaborative work with partners, it is important to note that the vision, development and direction of the investigation was that of the researcher. Finally, the contribution to knowledge and impact is discussed.

5.1 Maritime Ports and Cybersecurity

Output 1 (Kuhn et al., 2021b) uses desk-based research to review literature on ports and cybersecurity. It highlights ports as a cyber-physical environment and presents known cyber attacks in ports to illustrate the cyber-threat landscape. It then examines control mechanisms in place for cyber-risk management for ports and reviews current cybersecurity guidelines and standards. Lastly, it explores digital trends and the future of maritime ports and cybersecurity. The researcher designed Output 1, including the main conceptual ideas and the proof outline. She wrote the manuscript and oversaw the publication process, with the support of Ms. Kipkech. Prof. Shaikh supervised the project.

In the context of this thesis, Output 1 functions as the fulcrum between the researcher's previous work experience with maritime ports and the academic study of the environment. It was useful to apply a practical understanding of ports to the literature and enlightening to look at the industry from a new perspective. Choices made at this stage in the research journey include defining the scope for the rest of the theoretical and contextual framework by identifying gaps of knowledge to review in literature; to understand the complexity and challenges facing cybersecurity decision-making in the maritime sector, which relate to Research Objective 1 (Section 1.3). While vessels were touched upon, it became apparent they are key to understanding maritime cyber risk, especially in the context of increased connectivity, and additional information on them could offer more proficient insights. This established the scope for Output 2 (Kipkech et al., 2022).

Regarding contribution to knowledge, Output 1 fosters a new understanding of ports as cyber-physical environments which allows for the classification of cybersecurity attributes and cyber threat management. It presents five known cyber attacks that highlight the importance of cyber risk management in ports, and the need for a coordinated strategy. It also outlines the technological trends shaping the port industry and discusses cybersecurity implications of digital acceleration. Regarding contribution to impact, Output 1 influences the relevant disciplinary context of maritime cybersecurity and the wider field of practice; it was cited here (Karamperidis et al., 2021). It is also a resource for teaching purposes in academic programs, including as a scholar book for programs at the Maritime Academy of Asia and the Pacific (MAAP) (Associated Marine Officers' and Seamen's Union of the Philippines, 2022). The book was well received internationally; it has also been reviewed and promoted by international experts (Grzybowski, 2021).

5.2 Cyber Security and Disruptive Technologies

Output 2 (Kipkech et al., 2022) uses desk-based research to review literature on ship components and on maritime vessels as a cyber-physical environment. It presents known cyber attacks on vessels to develop an understanding of maritime cyber risk. It then examines efforts to overcome cyber threats to vessels and the role of cyber power in the maritime environment. It argues that the maritime sector has not demonstrated proportionate effort to understand cyber attacks, and therefore remains exposed to them. The researcher designed Output 2, including the main conceptual ideas and the proof outline along with Ms. Kipkech. The researcher wrote most of the manuscript with the support of Ms. Kipkech. Prof. Shaikh supervised the project.

In the context of this thesis, Output 2 further enhances an understanding of the complexity and challenges facing cybersecurity decision-making in the maritime sector, which relates to Research Objective 1 (Section 1.3), through examination of literature on vessels. Collectively, Outputs 1-2 establish a review of known cyber attacks in ports and on vessels which grounds this thesis and highlights its relevance. Further, conducting this review of literature also widened the researcher's knowledge of attacks in a manner that could later applied directly to the scenario writing in the first cybersecurity decision-making exercise, to ensure the scenarios maintained a high degree of ecological validity.

Choices made at this point in the research journey include defining the remaining scope for the theoretical and contextual framework by identifying the need to examine cyber insurance, which is '*'increasingly [...] a defining aspect of cyber risk management for maritime vessels"* (Kipkech et al., 2022). It became evident that additional information on cyber insurance could provide more proficient insights into current cyber risk management strategies. This set the agenda for the next output on cyber insurance (Kuhn et al., 2020b). Output 2 contributes to existing knowledge by developing an understanding of vessels as cyber-physical environments, allowing for the classification of cybersecurity attributes and cyber threat management. It presents eight cyber attacks that highlight the importance of cyber risk management in vessels. It also critically reviews cybersecurity frameworks as applicable to maritime vessels, along with their shortcomings, and discusses cyber power in the domain. Regarding contribution to impact, Output 2 is a resource for teaching purposes and influences the relevant disciplinary context of maritime cybersecurity and the wider field of practice.

5.3 Cyber Insurance and Risk Management: Challenges and Opportunities

Output 3 (Kuhn et al., 2020b) uses desk-based research to review literature on cyber insurance to develop an understanding of its associated challenges, including a lack of experience with cyber incidents, confusion around premiums, accumulated risk, missing metrics, and weak governance. It outlines resources which offer cybersecurity considerations and highlights the need for organisations to accurately model cyber risk. Output 3 resulted from significant discussion between collaborators, led by the researcher, on the topic of cyber insurance. She conceived of Output 3, including the main concepts, and wrote the manuscript with Dr. Vasudevan. Professor Carr supervised and added COVID-19 context into the introduction.

At this point in the research journey, the theoretical and contextual framework is established. While acknowledging the challenge of a lack of experience with cyber incidents, additional data gathering on cyber insurance rulings could have led to more proficient insights. For instance, in 2022 the pharmaceutical company Merck won cyber-insurance lawsuit in relation to 2017 NotPetya ransomware attack (Catalin Cimpanu, 2022).

Output 3 contributes to the existing knowledge base by offering relevant insights into the cyber insurance landscape and by examining the existing barriers to adopting cyber insurance. Cyber insurance is a mechanism that boards may deploy to deal with cyber risk, and it is a topic of relevance to industry. As cyber insurance is a relatively new tool and continues to evolve, Output 3 is exploratory in nature and aims to 'take the temperature' of the market in relation to cyber insurance, and to outline key take-aways. It identifies resources that exist which outline cybersecurity considerations and guide organisations thinking about taking out cyber insurance. Regarding impact, Output 3 contributes to dialogue between academic researchers and cybersecurity stakeholders, communicating a method to manage cyber risk in organisations. It may indirectly influence decisions of executives and influence organisational policy around cyber risk management.

5.4 Games for Cyber Security Decision-Making

Output 4 (Hussain et al., 2020) uses desk-based research to examine cybersecurity games and compiles a data-set of 46 games to investigate how effective such games are for assessing decision-making skills, and determines the state-of-the-art game. Through critical review and analysis of the data-set, a qualitative evaluation criteria to assess games for decision-making skills is presented. The criteria is then applied to ten games to determine the state-of-the-art game. It concludes with insights into how the assessment criteria can improve decision-making skills through games.

In the context of this thesis, Output 4 marks a shift in the research journey from constructing a theoretical and contextual framework to developing empirical knowledge. While it presents a data-set of games which may be considered within the context of Research Objective 1 (Section 1.3), it also develops a criteria to assess cybersecurity decision-making exercises for effectiveness, which relates to Research Objective 2 and which was used in the design of new cybersecurity decision-making exercises (Outputs 5-7). The researcher conceived the methodology along with Mr. Hussain and Prof. Shaikh. She carried out the survey, analysed and interpreted the results, and wrote the manuscript with Mr. Hussain. She presented at the conference. Prof. Shaikh supervised the project.

In Output 4, the analysis of game objectives revealed decision-making is an objective. Generally, technical and strategic decision-making are distinguished, but both are needed to develop a sufficient understanding of cybersecurity challenges to form an effective decision. The decision was taken at this point in the research journey not to discern between technical and strategic decision-making, since they happen simultaneously. This represents the complexities when exploring the human dimension of cybersecurity decision-making. Additionally, much consideration was given in the design of scenarios, with specific regard to the inclusion of 'injects' such as evidence, time pressure, escalation, reputation and resource allocation which trigger critical thinking and challenge decision-making. While the game objectives create an environment which frames decision-making, it is the scenario injects which trigger a response, critical thinking and challenge players to make decisions. However, of the ten games examined, almost all included game objectives centred around the themes that emerged, but incorporated less scenario injects. The decision was taken here to develop exercises with a greater focus on the use of scenario elements to provide more opportunities for decision-making. We acknowledge the criteria could also be refined through survey of more games. While 46 games informed this study, this could be extended to include a wider sample in which new trends may be incorporated into the criteria. For instance, the results are based on the available information only.

The contribution of Output 4 to knowledge is most clear in the identification of effective cybersecurity decision-making games. It provides insights into how assessment criteria can advance the development of better decision-making skills through games. It demonstrates the effectiveness of games to test and challenge both cybersecurity and decision-making skills. Regarding contribution to impact, Output 4 develops a criteria to assess cybersecurity games for decision-making, thus it adds value to the academic and cybersecurity game community- it was cited here (Mäses et al., 2021). It affirms games as an effective approach for strengthening cybersecurity decision-making.

5.5 Maritime Cyber Risk Perception and Response

Output 5 (Kuhn et al., 2020a) uses the simulation method to develop and test a cybersecurity decision-making exercise, to examine risk perception and response. Built on earlier work (Hussain et al., 2020), this exercise was undertaken by four participant groups which encountered three escalating scenarios that range over cyber incidents in the maritime domain. For each scenario, participants responded to four scenario inject cards to test decision-making. These are weighted according to the four response attributes to generate score (1-8) which was reported back to them at the end of the game. Results were analysed across groups. The findings highlight the importance of planning for cyberspace operations in the maritime environment, and lay the foundation for future research on cyber risk perception as a intricate governing factor in incident response. The researcher conceived of the idea, developed the methodology and planned the experiment. She led implementation of the experiment, independently analysed and interpreted the results, independently wrote the manuscript, and presented at the conference. Professor Shaikh and Professor Bicakci supported with implementation and reviewed the final manuscript.

Choices made at this point in the research journey include looking beyond the board.

While the cybersecurity decision-making exercise was designed for board members, the scope of exercise participants was expanded to include executive decision-makers. This was due to difficulty in recruiting board members and also due to the realisation that cybersecurity decision-making extends beyond the board. The expanded scope of participants better captures the intricacies involved in addressing cyber risk in an organisation, whereby responsibility is often split. Cyber preparedness should be undertaken by many players, and thus the focus should include the interplay of communication and responsibilities between roles. Regarding where further data collection could have led to more insights, it would have been interesting to recruit participants from one organisation to be able to draw insights into a specific organisational security culture. It would have also been useful to link background data gathered from participants to their group responses, to draw insights on the aggregated experience and expertise of each group.

Output 5 contributes to existing knowledge by demonstrating that effective assessment of cyber risk perception can be done by calibrating risk, according to relevant guidelines, in a group setting. Further, the findings may provide insights into groups with significant public/military sector experience (more than five years): Output 5 suggests that as incident impact rises, groups with strong public/military sector experience and mixed cybersecurity expertise respond in favour of private sector responsibility and visibility, but not in favour of urgency or directness. Regarding contribution to impact, this exercise, trialled successfully in small setting, offers insights into how games can build capacity and echoes the need for joint response. They may be used to explore tendencies which characterise the security culture of North Atlantic Treaty Organization (NATO) and an emerging common risk perception. It is a tool for NATO partners to prepare and plan cyberspace operations in the maritime environment. Further, 68 cybersecurity experts across NATO member states were able to potentially improve capacity for cybersecurity decision-making by participating in this exercise.

5.6 COVID-19 Digitisation in Maritime: Understanding Cyber Risks

Output 6 (Kuhn et al., 2021a) uses the simulation method to develop and test a cybersecurity decision-making exercise (detailed in the previous output). The discussion is focused around digital acceleration and its implications for maritime cyber risk. As maritime organisations embrace accelerated digitisation due to COVID-19, they must take steps to prevent and defend against cyber threats. This exercise presents a tool to prepare robust cyberspace operations and contextualises it. The researcher conceived of the idea, developed the methodology, planned the experiment and led its implementation. She analysed and interpreted the results, and wrote the manuscript. Prof. Shaikh and Prof Bicakci supported the implementation. Prof. Shaikh supervised the project.

Choices made at this point of the research journey include the decision to calibrate the expert. As the exercise participants are executive decision-makers, many with invaluable experience working with cyber risk in a professional setting, this thesis considers them the experts in the room. While many exercises aim to offer recommendations or to rate their participants, this research acknowledges that succeeding or not as an executive decision-maker is best judged by the organisation they are employed by. Each organisation has a unique risk appetite and risk culture, which means there is no across-the-board answer. This exercise aims not to offer recommendations back to decision-makers but rather to gauge their individual response tendencies against themselves- as a group. Thus, it aims to calibrate the expert under the belief that when decision-makers who work together share the same risk perception, they can improve cyber readiness. Further, while the trends in Figure 10 on page 53 are interpreted through participant data (experience and expertise), we acknowledge that the exercise may benefit from the collection of more background data from which to interpret the results (to capture the ‘why’ behind the tendencies). This change was incorporated in Exercise 2, detailed in Output 7 (Parkin et al., 2021).

Output 6 contributes to existing knowledge by analysing key implications of digital acceleration on maritime cybersecurity and investigating collective cyber risk perception–

and how this may impact response. It evidences that COVID-19 has led to greater reliance on technology and has produced new digital opportunity structures that increase cyber risk. It highlights the need to plan for cyberspace operations and grounds cyber risks as a intricate governing factor in maritime. Regarding contribution to impact, Output 6 presents an exercise which may be used as a training tool for actors across the maritime community, including industry, government, and international organisations, to challenge risk perceptions and to strengthen a shared security culture. The research community can benefit from Output 6 by incorporating cybersecurity decision-making exercise environments in their research. It has been cited in seven academic publications (Ben Farah et al., 2022; Ichimura et al., 2022; Balavenu et al., 2022; Veerasamy et al., 2022; Karim, 2022; Kanwal et al., 2022; Vanelslander, 2022).

5.7 Scenario-Driven Assessment of Cyber Risk Perception at the Security Executive Level

Output 7 (Parkin et al., 2021) explores a much under-researched area – perceptions of cybersecurity and cyber risk at the highest levels of an organisation — and uses the simulation method to develop and test a new cybersecurity decision-making exercise. In many ways, it is an improved version of Exercise 1, upon which the researcher was able to reflect on and incorporate new elements. This includes, for instance, the introduction of the Cambridge Taxonomy of Business Risks (Cambridge Centre for Risk Studies, 2019) to gauge the participants' perception and assessment of many organisational risks which could be posed by a cyber incident. Such improvements illustrate the value of continuing to develop such exercises, which can be tailored to the participants and refined to better assess and improve executive cybersecurity decision-making. Output 7 explores why cyber risk perception is an important but challenging concept. It then demonstrates an approach to risk articulation, in terms of systematically constructed scenarios, and assesses whether this resonates with decision-makers. As part of this, it assesses cybersecurity decision-makers for their perception of wider business risks and stakeholders. The researcher conceived of the idea and developed the methodology with Prof. Shaikh and Dr. Parkin. She and Prof. Shaikh planned and implemented the simulation. The researcher analysed and interpreted the results. She worked with Prof. Shaikh and Dr. Parkin to write the manuscript. Dr. Parkin presented at the conference.

Choices made at this point of journey include the decision to explore risks that extend beyond cyber, whereby cyber incidents pose many business risks for organisations due to their complexity. To include a wider scope of risks, this exercise adopts the Cambridge Taxonomy of Business Risks (Cambridge Centre for Risk Studies, 2019). In this way, the research explores more fully how executive decision-makers perceive risks associated with cyber incidents, and also how they might prioritise various business risks. The opportunity to improve Exercise 2 is acknowledged (Parkin et al., 2021), whereby although wider business risks were considered only cyber-risk managers were engaged. It would have been interesting to involve a range of stakeholders in the same exercise, as cyber-related decisions are not only about ‘cyber’ and require coordination with others within and outside of the organisation. Further, as the scenarios were designed to include 3, 4, and 5 risks (See “Anticipated Risks” in Figure 6 on page 44), there may be scope to improve Exercise 2 by more clearly articulating risk in the scenarios (in particular, S2 and S3 where the participants on average perceived 2.84 (S2) and 3.63 (S3) risk categories, as shown in Figure 13 on page 59. Yet, the general trend of increased risks was captured by the group.

Regarding knowledge contribution, this output establishes clarity on how executive decision-makers support wider business to respond to cyber attacks and it develops a structured, scenario-driven and repeatable exercise for them. Regarding contribution to impact, organisations can benefit from Output 7 findings by incorporating cybersecurity decision-making exercise environments in their training, to challenge risk perceptions and strengthen a shared security culture. Further, 19 CIOs and IT managers potentially improved their capacity for cybersecurity decision-making by participating in this exercise. It has been cited in two academic publications (Larsen et al., 2022; Tomlinson et al., 2022).

Chapter 6

Conclusion

The main aim of this research was to develop new approaches that enhance the understanding of cybersecurity risks at the senior leadership level in organisations. This aim has been fulfilled by completing four core objectives that were designed to (1) develop an understanding of the risks, impacts and other associated challenges influencing cybersecurity decision-making in the maritime domain; (2) analyse the most effective methods for simulation-based approaches in cybersecurity; (3) develop, test and apply scenario-driven exercises for executive decision-makers to understand cybersecurity risks and decision-making processes; and (4) establish the potentiality of game-based learning for raising awareness of cyber risks at the senior executive level. This chapter brings all of the research together, concludes on the key findings from the research, and presents potential future areas of research based on these findings.

6.1 Key Findings

The research has established many findings for cybersecurity decision-making in the maritime domain and how the use of game-based learning can benefit this. That said, three key findings emerged which relate to (1) the principal risks, impacts and challenges for cybersecurity decision-making, (2) game-based simulation as the most effective method for simulation-based approaches in cybersecurity, and (3) insights about cybersecurity risks and decision-making processes for executive decision-makers.

First, in addressing Research Objective 1 (Section 1.3), the literature review develops an understanding of the risks, impacts and challenges influencing cybersecurity decision-making in the maritime domain. Through examining known cyber attacks on ports and vessels, key risks were found to involve the probability of a threat agent exploiting a vulnerability to harm a computer, network, system or utility. Insight was also gained about the impacts associated with such attacks, which may include loss, injury, catastrophe or other undesirable outcomes- such as disruption or damage to an organisation's reputation. Developing an understanding of risks and impacts was important as it provided context to ground the research, for example the attacks examined later informed the written exercise scenarios. This also led to an understanding of challenges influencing cybersecurity decision-making in the domain, whereby maritime cyber risk is complex, evolving, and asymmetrical; larger attack surfaces, greater uncertainty, and interconnected operations (due to digitisation, automation, information networks and integrated systems) makes it hard to assess risk and formulate response. In this this way, the thesis expands an existing body of research to establish decision-making as a key governing factor in what informs senior executives' response to cybersecurity incidents. It establishes that, despite its weight, the maritime sector has not demonstrated proportionate effort to understand cyberattacks, and therefore remains exposed to them. This is a call to action: *"It is imperative to act with urgency and purpose to protect the cyber domain from crippling attacks and disruption"* (Kuhn et al., 2021b). The understanding of ports and vessels as cyber–physical environments provided in this thesis paves the way for the future classification of cybersecurity attributes and the management of cyber risks.

Second, in answering Research Objective 2 (Section 1.3), the literature review identified game-based simulation as the most effective method for simulation-based approaches in cybersecurity. While this method raises inherent validity considerations, it allows for the study of interactions of a complex systems and it enables experimentation with new designs or policies before implementation, which makes it suitable to understand and prepare how an organisation might respond to a complex cyber incident. Where the subjective nature of decision-making necessitates a method that allows for the contextualisation of data (the 'why') to be able to assess effectiveness, this method allows in-depth investigation which makes it suitable for a study focused on decision-making around a cyber incident. However, it also allows the researcher to collect lots of information from a group in a short time (focus group discussions), and offers participants flexibility. This was key given the difficulty in recruiting executive decision-makers and COVID-19-related social distancing measures. To address the inherent validity considerations, where it is challenging to mimic forces that motivate participants' drive to complete a task and to mimic risks which may inform their decision-making, scenario design was informed by known cybersecurity incidents that affected organisations.

Third, in addressing Research Objective 3 (Section 1.3), the research developed, tested, and applied two scenario-driven exercises for executive decision-makers which offered insights about cybersecurity risks and decision-making processes. It demonstrates that risk assessment for executive decision-makers may be gauged in two ways. First, by assessing participants' ability to accurately perceive incident severity. This includes comparing perceived incident severity against actual incident severity (of escalating scenarios) to indicate the proportionality of their response. Second, by assessing participants' ability to perceive wider business risks associated with cyber incidents. This indicates their ability to correctly identify risks, whereas risk identification is a key competence of effective decision-making. In gauging risk assessment for executive decision-makers in these ways, this research demonstrates that executive decision-makers perceive wider business risks associated with a cyber incident, which is important because it indicates risk awareness. Further, it captures how these risks are prioritised and the 'why' behind this, as well as capturing areas of uncertainly and technical complexity, which together offer important insights into the perceived implications of a risk, so we might understand 'why' a decision was taken. For instance, in Exercise 2 a participant perceived the implication of *"cascading risk"* which indicates they understood the complexities posed by this scenario. Finally, by assessing and calibrating tendencies across a group, we gain insights through which may understand the group's risk perception, which is important because if offers insights into a group's risk appetite/ security culture.

Through the above findings, this thesis accomplishes the final research objective (Section 1.3) by establishing the potentiality of game-based learning for raising awareness of cyber risks at the senior executive level. Senior executives can benefit from insights drawn from their decision-making process. They have much to gain from further developments in the field cybersecurity decision-making, with specific regard to training and capacity building exercises.

6.2 Contribution of the Research

In developing approaches for enhancing the understanding of cybersecurity risk at the senior leadership level in organisations, this thesis makes three original research contributions to the disciplines of maritime, cybersecurity, and decision-making, which relate to (1) providing new approaches, evidence and insights for closing the gap in extant literature, whereby a review of the extant literature base has not identified a body of knowledge focused on cybersecurity decision-making at the senior leadership level utilising scenario-based approaches; (2) researching and developing methods and approaches for supporting decision-making in the context of cybersecurity incidents, cyber risks and consequently cyber readiness, and; (3) testing and validating these methods and approaches to highlight the potentiality of simulation-based approaches for enhancing decision-making.

Through the adoption of this research by senior executives, maritime stakeholders, researchers and others, this thesis answers the need for further cybersecurity training tools within the maritime community, to reinforce proportionate response to cyber incidents. Maritime organisations and stakeholders can benefit from the findings of this research through the application of a new understanding of the current cyber threat landscape and by incorporating cybersecurity decision-making game environments in their training, to challenge executive decision-makers and their risk perceptions, ultimately strengthening a shared security culture.

6.3 Future Research Opportunities

Future work in cybersecurity decision-making can provide further understanding and significant benefit to senior executives in the maritime domain. Most obviously, this includes replication of the exercises in maritime organisations where *"There is a great need for cybersecurity training tools within the maritime community that reinforce proportionate response to cyber incidents"* (Kuhn et al., 2021a). As suggested by the word "reinforce", further iterations of the game may serve to strengthen the findings of the study. Rather than measuring their results against an external benchmark, the group response as a whole is used to validate response. The value of this measurement increases with the number of participants who take part in the exercise—leading to greater calibration, which is a clear direction for future research. Likewise, the criteria presented in this research could be refined through the survey of more games. While 46 games informed this research, this could be extended to include a wider sample from which new trends may emerge.

The exercises presented in the research can also be refined through further research. A lesson to draw here relates to the process of scenario writing, whereby the perception of risk may also be informed by the choice of terminology used in the research exercise (Krol et al., 2016) and nuances hiding in the narrative. Future applications of the approach will involve consultation with knowledgeable external experts to assess scenario content for particular participant groups. In terms of scenario content, aspects of organisational behaviour, such as media attention or dependence on suppliers, may be more tangible dimensions along which to escalate scenarios. As such, these notions may allow for calibration of participants' skills and experience against expected identification of risks, where accounting for the biases of the decision-makers is key in objectively managing business risks (Hubbard and Drummond, 2011). Regarding how executives **"deal with risk"** (Shapira, 1995), the recognition of various risk types by security executives paradoxically highlights that cyber-risk management in organisations is not the sole responsibility of executives. Distributed decision-making is observed elsewhere (M'manga, 2020); decisions at the executive level may further involve two-way sharing of information so that security and top management objectives are both met. Cyber-risk management is also not an activity to be pursued unilaterally by organisations as indicated elsewhere (Moore et al., 2015), where security features in perspectives on general business risks (Bagri, 2019). Future work can involve a range of stakeholders in similar exercises – cyber-related decisions are not only about 'cyber', requiring coordination with many others in and out of the organisation.

Bibliography

Adkins, S. (2019). Revenues for Global Game-based Learning Will Surge to Over $24 Billion by 2024. *Cision PR Web*. https://www.prweb.com/releases/revenues_for_global_game_based_learning_will_surge_to_over_24_billion_by_2024/prweb16424728.htm.

Al Jazeera Media Network (2020). Israel cyberattack caused 'total disarray' at iran port: Report. https://www.aljazeera.com/news/2020/5/19/israel-cyberattack-caused-total-disarray-at-iran-port-report.

Amigud, A., Arnedo-Moreno, J., Daradoumis, T., and Guerrero-Roldan, A.-E. (2018). An integrative review of security and integrity strategies in an academic environment: Current understanding and emerging perspectives. *Computers & Security*, 76:50–70.

Antonucci, D. (2017). *The cyber risk handbook: creating and measuring effective cybersecurity capabilities*. John Wiley & Sons.

Associated Marine Officers' and Seamen's Union of the Philippines (2022). Maritime Academy of Asia and the Pacific (MAAP). https://maap.edu.ph/.

Atlantic Council (2019). The Cyber 9/12 UK Strategy Challenge. Technical report. https://www.cyber912uk.org/en/.

Bagri, P. (2019). The multidimensionality of business risk: A managerial perspective implications for its classification, interpretation & management. *Singapore Management University: Dissertations and Theses Collection (Open Access)*. https://ink.library.smu.edu.sg/etd_coll/206/.

Balavenu, R., Khan, A. K., Faisal, S. M., Sriprasadh, K., and Sisodia, D. R. (2022). An empirical investigation in analysing the proactive approach of artificial intelligence in regulating the financial sector. In *International Conference on Emerging Technologies in Computer Engineering*, pages 90–98. Springer.

Banks, J., Carson II, J., Nelson, B., and Nicol, D. (2005). *Discrete-event system simulation, fourth edition*. Pearson.

Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., and Bellekens, X. (2022). Cyber security in the maritime industry: a systematic survey of recent advances and future trends. *Information*, 13(1):22.

BIMCO (2018). The Guidelines on Cyber Security Onboard Ships, Version 3. https://www.american-club.com/files/files/Guidelines_on_Cyber_Security_Onboard_Ships_v3.pdf,.

Cambridge Centre for Risk Studies (2019). Global Risk Index 2020 Executive Summary. https://www.jbs.cam.ac.uk/wp-content/uploads/2021/11/crs-cambridge-global-risk-index-2020.pdf.

Caralli, R. A., Stevens, J. F., Young, L. R., and Wilson, W. R. (2007). Introducing octave allegro: Improving the information security risk assessment process. Technical report, Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, 92(1):43–62.

Catalin Cimpanu (2022). Merck wins cyber-insurance lawsuit related to notpetya attack. *The Record*. https://therecord.media/merck-wins-cyber-insurance-lawsuit-related-to-notpetya-attack/.

Chittaro, L. and Buttussi, F. (2015). Assessing knowledge retention of an immersive serious game vs. a traditional education method in aviation safety. *IEEE Transactions on Visualization and Computer Graphics*, 21(4):529–538.

Creswell, J. W. (1994). Qualitative and quantitative approaches. *Sage Publications*.

Creswell, J. W. (2002). Educational research: Planning, conducting, and evaluating quantitative and qualitative research. Merrill Prentice-Hall. *Theory into Practice*, 39(3):124–130.

Creswell, J. W. (2009). Research design-qualitative, quantitative, and mixed methods approaches (3rd ed.). *Sage Publications.*

Creswell, J. W. (2017). *Research design: Qualitative, Quantitative, and Mixed Methods Approaches.* Sage publications.

Creswell, J. W., Plano Clark, V. L., Gutmann, M. L., and Hanson, W. E. (2003). Advanced mixed methods research designs. *Handbook of mixed methods in social and behavioral research*, pages 209–240.

Crookall, D. (2000). Thirty years of interdisciplinarity. *Simulation & Gaming*, 31(1):5–21.

Crotty, M. (2020). *The foundations of social research: Meaning and perspective in the research process.* Routledge.

Cyberhedge (2020). World's second largest container shipping company msc suffers a network outage, possibly due to a cyber attack. https://cyberhedge.com/insights/daily/2020/04/14/world-s-second-largest-container-shipping-company-msc-suffers-a-network-outage-possibly-due-to-a-cyber-attack/.

Daffron, J., Ruffle, S., Coburn, A., Copic, J., Quantrill, K., Strong, K., and Leverett, E. (2019). Shen attack: Cyber risk in asia pacific ports. *Centre for Risk Studies, Cambridge.*

De Smidt, G. and Botzen, W. (2018). Perceptions of corporate cyber risks and insurance decision-making. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 43(2):239–274.

Dittrich, D., Kenneally, E., et al. (2012). The menlo report: Ethical principles guiding information and communication technology research. Technical report, US Department of Homeland Security.

Dooley, K. (2017). Simulation research methods. *The Blackwell companion to organizations*, pages 829–848.

Erlingsson, C. and Brysiewicz, P. (2017). A hands-on guide to doing content analysis. *African journal of emergency medicine*, 7(3):93–99.

European Commission (2018). 2018 reform of EU data protection rules. https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf.

Fiveash, K. (2019). The Norsk Hydro cyber attack is about money, not war. https://www.wired.co.uk/article/norsk-hydro-cyber-attack.

Frey, S., Rashid, A., Anthonysamy, P., Pinto-Albuquerque, M., and Naqvi, S. A. (2017). The good, the bad and the ugly: a study of security decisions in a cyber-physical systems game. *IEEE Transactions on Software Engineering*, 45(5):521–536.

Goldsmith, J. (2013). How cyber changes the laws of war. *European Journal of International Law*, 24(1):129–138.

Gomez, M. A. and Whyte, C. (2022). Cyber uncertainties: Observations from cross-national war games. In *Cyber Security Politics*, pages 111–127. Routledge.

Grasso Macola, I. (2020). US Tugboat cyber-attack: the experts respond. https://www.ship-technology.com/features/cyber-attacks-in-the-maritime-sector-the-experts-respond/.

Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Growth Engineering (2020). What is Game-based Learning? https://www.growthengineering.co.uk/what-is-game-based-learning/.

Grzybowski, M. (2021). Digitization in sea ports and maritime transport. Full steam ahead.

https://www.marinepoland.com/seaports-shipping-logistics-digitization-in-sea-ports-and-maritime-transport-full-steam-ahead-1391.

Habash, R., Groza, V., and Burr, K. (2013). Risk management framework for the power grid cyber-physical security. *British journal of applied science & technology*, 3(4):1070–1085.

Haggman, A. (2019). *Cyber Wargaming: Finding, Designing, and Playing Wargames for Cyber Security Education.* PhD thesis, Royal Holloway, University of London.

Healey, J. (2017). Who's in control: Balance in cyber's public-private sector partnerships. *Georgetown Journal of International Affairs*, 18:120.

Hennink, M., Hutter, I., and Bailey, A. (2020). *Qualitative research methods.* Sage.

Horne, R. (2017). Governing cyber security risk: It's time to take it seriously: Seven principles for Boards and Investors. https://www.pwc.co.uk/cyber-security/assets/governing-cyber-security-risk.pdf.

Hubbard, D. W. (2020). *The failure of risk management: Why it's broken and how to fix it.* John Wiley & Sons.

Hubbard, D. W. and Drummond, D. (2011). *How to measure anything.* Wiley Online Library.

Hussain, A., Kuhn, K., and Shaikh, S. (2020). Games for cybersecurity decision-making. In *Fang, X. (eds) HCI in Games. HCII 2020. Lecture Notes in Computer Science, vol 12211*, pages 411–423. Springer.

Ichimura, Y., Dalaklis, D., Kitada, M., and Christodoulou, A. (2022). Shipping in the era of digitalization: Mapping the future strategic plans of major maritime commercial actors. *Digital Business*, 2(1):100022.

International Chamber of Shipping (2020). Shipping and World Trade. https://www.ics-shipping.org/shipping-facts/shipping-and-world-trade.

International Maritime Organization (2017). Msc-fal.1/circ.3 guidelines on maritime cyber risk management. https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

International Maritime Organization (2019). Strategy for the Development and Implementation of E-Navigation. https://www.imo.org/en/OurWork/Safety/Pages/eNavigation.aspx.

Jalali, M. S., Siegel, M., and Madnick, S. (2019). Decision-making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment. *The Journal of Strategic Information Systems*, 28(1):66–82.

Johnson, C. W. (2008). Using evacuation simulations for contingency planning to enhance the security and safety of the 2012 olympic venues. *Safety science*, 46(2):302–322.

Kanwal, K., Shi, W., Kontovas, C., Yang, Z., and Chang, C.-H. (2022). Maritime cybersecurity: are onboard systems ready? *Maritime Policy & Management*, pages 1–19.

Karamperidis, S., Kapalidis, C., and Watson, T. (2021). Maritime cyber security: A global challenge tackled through distinct regional approaches. *Journal of Marine Science and Engineering*, 9(12):1323.

Karim, M. S. (2022). Maritime cybersecurity and the imo legal instruments: Sluggish response to an escalating threat? *Marine Policy*, 143:105138.

Kaspersky (2019). Kaspersky Interactive Protection Simulation. Technical report. https://media.kaspersky.com/en/business-security/enterprise/KL_SA_KIPS_overview_A4_Eng_web.pdf.

Kaspersky Inc. (2021). Kaspersky Interactive Protection Simulation. https://media.kaspersky.com/en/business-security/enterprise/KL_SA_KIPS_overview_A4_Eng_web.pdf.

Kelion, L. (2020). Blackbaud: Bank details and passwords at risk in giant charities hack. *BBC*. https://www.bbc.com/news/technology-54370568.

Kipkech, J., Kuhn, K., and Shaikh, S. (2022). Cyber security and disruptive technologies. In *Routledge Handbook of Maritime Security*, pages 214–226. Routledge.

Konrad, J. (2020). IMO Cyber-attack Has Serious Implications. https://gcaptain.com/imo-cyberattack-has-serious-implications/.

Krol, K., Spring, J. M., Parkin, S., and Sasse, M. A. (2016). Towards robust experimental design for user studies in security and privacy. In *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2016)*, pages 21–31.

Kuhn, K. (2022a). Data-set for cybersecurity decision-making exercise 1. https://pureportal.coventry.ac.uk/en/datasets/data-set-for-cybersecurity-decision-making-exercise-1.

Kuhn, K. (2022b). Data-set for cybersecurity decision-making exercise 2. https://pureportal.coventry.ac.uk/en/datasets/data-set-for-cybersecurity-decision-making-exercise-2.

Kuhn, K., Bicakci, S., and Shaikh, S. (2020a). Maritime cyber risk perception and response. In *4th NMIOTC Conference on Cybersecurity in the Maritime Domain*, pages In–Press. https://nmiotc.nato.int/pressreleases/4th-cyber-security-conference-in-maritime-domain/.

Kuhn, K., Bicakci, S., and Shaikh, S. (2021a). Covid-19 digitization in maritime: understanding cyber risks. *WMU Journal of Maritime Affairs*, 20(2):193–214.

Kuhn, K., Kipkech, J., and Shaikh, S. (2021b). Maritime ports and cybersecurity. In *Maritime Transport and ITS Solutions in Port Logistics*, pages 37 – 67. Institution of Engineering and Technology.

Kuhn, K., Vasudevan, S., and Carr, M. (2020b). Cyber insurance and risk management: Challenges and opportunities. *Research Institute for Sociotechnical Cyber Security*. https://www.riscs.org.uk/cyber-insurance/.

Lam, J. and Su, S. (2015). Disruption risks and mitigation strategies: an analysis of Asian ports. *Maritime Policy & Management*, 42(5):415–435.

Larsen, M. H., Lund, M. S., and Bjørneseth, F. B. (2022). A model of factors influencing deck officers' cyber risk perception in offshore operations. *Maritime Transport Research*, 3:100065.

Lee, Y.-I., Trim, P., Upton, J., and Upton, D. (2009). Large emergency-response exercises: Qualitative characteristics-a survey. *Simulation & gaming*, 40(6):726–751.

Lété, B. and Pernik, P. (2017). *EU-NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions*. German Marshall Fund of the United States.

Marsh LLC and Microsoft (2019). 2019 global cyber risk perception survey. Technical report, Marsh LLC and Microsoft. https://www.marshmclennan.com/insights/publications/2019/sep/global-cyber-risk-perception-survey-report-2019.html.

Mäses, S., Maennel, K., Toussaint, M., and Rosa, V. (2021). Success factors for designing a cybersecurity exercise on the example of incident response. In *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 259–268. IEEE.

Massie, R. (2015). *Allocating effort: risk and complexity in board directors' engagement with information*. PhD thesis, City University London.

Mazumdar, T., Raj, S. P., and Sinha, I. (2005). Reference price research: Review and propositions. *Journal of marketing*, 69(4):84–102.

Moore, T., Dynes, S., and Chang, F. R. (2015). Identifying how firms manage cybersecurity investment. *Southern Methodist University*, 32. http://blog.smu.edu/research/files/2015/10/SMU-IBM.pdf.

Morse, A. (2018). Investigation: WannaCry cyber attack and the NHS. *National Audit Office*. https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/.

M'manga, A. (2020). *Designing for cyber security risk-based decision making.* PhD thesis, Bournemouth University.

National Cyber Security Centre (2018). New cyber attack categorisation system to improve UK response to incidents. https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents,.

National Cyber Security Centre (2019). Board Toolkit. https://www.ncsc.gov.uk/collection/board-toolkit.

National Institute of Standards and Technology (2018). Framework for improving critical infrastructure cybersecurity. Technical report. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Nordberg, D. and Booth, R. (2018). Evaluating the effectiveness of corporate boards. *Corporate Governance: International Journal of Business in Society*, 19(2):372–387.

North Atlantic Treaty Organization (NATO) (2020). Statement by the north atlantic council concerning malicious cyber activities. https://www.nato.int/cps/en/natohq/official_texts_176136.htm.

Ogee, A., Gavrila, R., Trimintzios, P., Stavropoulos, V., and Zacharis, A. (2015). The 2015 Report on National and International Cyber Security Exercises: Survey, Analysis and Recommendations. *European Union Agency for Network and Information Security (ENISA).* https://op.europa.eu/en/publication-detail/-/publication/b09c680b-a2f7-11e5-b528-01aa75ed71a1/language-en.

Ouzounis, E., Trimintzios, P., and Saragiotis, P. (2009). National Exercise - Good Practice Guide. Technical report, European Network and Information Security Agency (ENISA). https://www.enisa.europa.eu/publications/national-exercise-good-practice-guide.

Pallas, F. (2009). Information security inside organizations-a positive model and some normative arguments based on new institutional economics. *SSRN 1471801:*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1471801.

Parkin, S., Kuhn, K., and Shaikh, S. (2021). Scenario-driven assessment of cyber risk perception at the security executive level. In *Workshop on Usable Security and Privacy*, pages In–Press.

Pearlson, K., Thorson, B., Madnick, S., and Coden, M. (2021). Cyberattacks are inevitable. is your company prepared? *Harvard Business Review*. https://hbr.org/2021/03/cyberattacks-are-inevitable-is-your-company-prepared.

Reinfelder, L., Landwirth, R., and Benenson, Z. (2019). Security managers are not the enemy either. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–7.

Rhee, H.-S., Ryu, Y. U., and Kim, C.-T. (2012). Unrealistic optimism on information security management. *Computers & Security*, 31(2):221–232.

Robbins, P. and Aydede, M. (2008). *The Cambridge handbook of situated cognition*. Cambridge University Press.

Rogers, G. O. (1984). Residential proximity, perceived and acceptable risk. In *Low-Probability High-Consequence Risk Analysis*, pages 507–520. Springer.

Salen, K. and Zimmerman, E. (2004). *Rules of play: Game design fundamentals*. MIT press.

Sanchez-Rodrigues, V., Potter, A., and Naim, M. (2010). Evaluating the causes of uncertainty in logistics operations. *The International Journal of Logistics Management*, 21(1):45–64.

Schechter, S. (2013). Common pitfalls in writing about security and privacy human subjects experiments, and how to avoid them. *Microsoft Research*.

Shapira, Z. (1995). *Risk taking: A managerial perspective*. Russell Sage Foundation.

Shen, C. and Baker, J. (2020). CMA CGM confirms ransomware attack. *Lloyd's List.* https://lloydslist.maritimeintelligence.informa.com/LL1134044/CMA-CGM-confirms-ransomware-attack.

Shreeve, B., Hallett, J., Edwards, M., Anthonysamy, P., Frey, S., and Rashid, A. (2020). "So If Mr Blue Head Here Clicks the Link..." Risk Thinking in Cyber Security Decision Making. *ACM Trans. Priv. Secur.*, 24(1).

Shreeve, B., Hallett, J., Edwards, M., Ramokapane, K. M., Atkins, R., and Rashid, A. (2020). The best laid plans or lack thereof: Security decision-making of different stakeholder groups. *IEEE Transactions on Software Engineering*, pages 1–1.

Smith, D. and Elliott, D. (2007). Exploring the barriers to learning from crisis: Organizational learning and crisis. *Management Learning*, 38(5):519–538.

Smith, J., Doody, K., and Veitch, B. (2019). Being prepared for emergencies: a virtual environment experiment on the retention and maintenance of egress skills. *WMU Journal of Maritime Affairs*, 18(3):425–449.

Smith, R. (2010). The long history of gaming in military training. *Simulation & Gaming*, 41(1):6–19.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of business research*, 104:333–339.

Stake, R. (2000). Case studies. In *N.K. Denzin and Y.S. Lincoln (Eds.), Handbook of qualitative research (2nd ed.)*, pages 435–454. Sage Publications.

Tam, K. and Jones, K. (2018). Cyber-risk assessment for autonomous ships. In *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pages 1–8. IEEE.

Tam, K. and Jones, K. (2019). Macra: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, 18(1):129–163.

Tanczer, L., Steenmans, I., Brass, I., and Carr, M. (2018). Networked world: Risks and opportunities in the internet of things. *Lloyd's of London*. https://discovery.ucl.ac.uk/id/eprint/10063068/1/InterconnectedWorld2018.pdf.

Tioh, J., Mina, M., and Jacobson, D. W. (2017). Cyber Security Training a Survey of Serious Games in Cyber Security. In *2017 IEEE Frontiers in Education Conference (FIE)*, pages 1–5.

Tomlinson, A., Parkin, S., and Shaikh, S. A. (2022). Drivers and barriers for secure hardware adoption across ecosystem stakeholders. *Journal of Cybersecurity*, 8(1):1–14.

Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human resource development review*, 4(3):356–367.

Twining, G. (2020). MSC Confirm Malware Attack. https://safetyatsea.net/news/2020/msc-confirm-malware-attack/.

Vanelslander, T. (2022). Short-run impacts of covid-19 on the maritime and port sector: measures and recommended policies. In *Transportation amid pandemics: practices and policies*, pages In–Press.

Veerasamy, K., Sanyal, S., Almahirah, M. S., Saxena, M., and Manohar Bhanushali, M. (2022). An investigative analysis for iot based supply chain coordination and control through machine learning. In *International Conference on Emerging Technologies in Computer Engineering*, pages 149–159. Springer.

VesselFinder (2022). . https://www.vesselfinder.com/?imo=9811000.

Walker, W. E. (1995). *The use of scenarios and gaming in crisis management planning and training*, volume 7897. Rand.

Weinstein, D. (2019). America's cyber blind spot. *The Hill*. https://thehill.com/opinion/cybersecurity/461452-americas-cyber-blind-spot/.

Whitton, N. (2012). Games-based learning. In *Encylopedia of the sciences of learning*, pages 1337–1340. Springer Nature.

Wiese Bockmann, M. (2019). Seized uk tanker likely 'spoofed' by iran. https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran.

Williams, M. J. (2008). *NATO, security and risk management: from Kosovo to Khandahar*. Routledge.

Wingrove, M. (2020). Toll suffers second cyber attack in four months. *Riviera Maritime Media*. https://www.rivieramm.com/news-content-hub/news-content-hub/toll-suffers-second-cyber-attack-in-four-months-59287,.

Wisker, G. (2007). *The postgraduate research handbook: Succeed with your MA, MPhil, EdD and PhD*. Macmillan International Higher Education.

Wisker, G. (2018). *The undergraduate research handbook*. Macmillan International Higher Education.

World Economic Forum (2020). The Global Risks Report 2020. https://reports.weforum.org/global-risks-report-2020/.

Appendices

Annex A

Summary of Outputs

2021

Kuhn, K., Bicakci, S., and Shaikh, S. (2021). Covid-19 digitization in maritime: understanding cyber risks. *WMU Journal of Maritime Affairs,* 20(2):193–214.
DOI: 10.1007/s13437-021-00235-1.
Co-authored journal article, peer-reviewed

Parkin, S., Kuhn, K. & Shaikh S. (2021) Scenario-Driven Assessment of Cyber Risk Perception at the Security Executive Level. In *Workshop on Usable Security and Privacy*, pages In–Press.
http://www.usablesecurity.net/USEC/usec21/papers/usec2021_Simon_Parkin.pdf.
Co-authored conference proceeding, peer-reviewed

Kipkech, J., Kuhn, K. & Shaikh, S. (2022) Cyber Security and Disruptive Technologies. In *Routledge Handbook of Maritime Security*, pages 214-226. Routledge.
ISBN: 978-0367430641.
Co-authored book chapter, peer-reviewed

Kuhn, K., Kipkech, J. & Shaikh, S. (2021) Maritime Ports and Cybersecurity. In *Maritime Transport and ITS Solutions in Port Logistics*, pages 37–67. Institution of Engineering and Technology.
ISBN: 978-1-83953-086-9.
Co-authored book chapter, peer-reviewed

2020

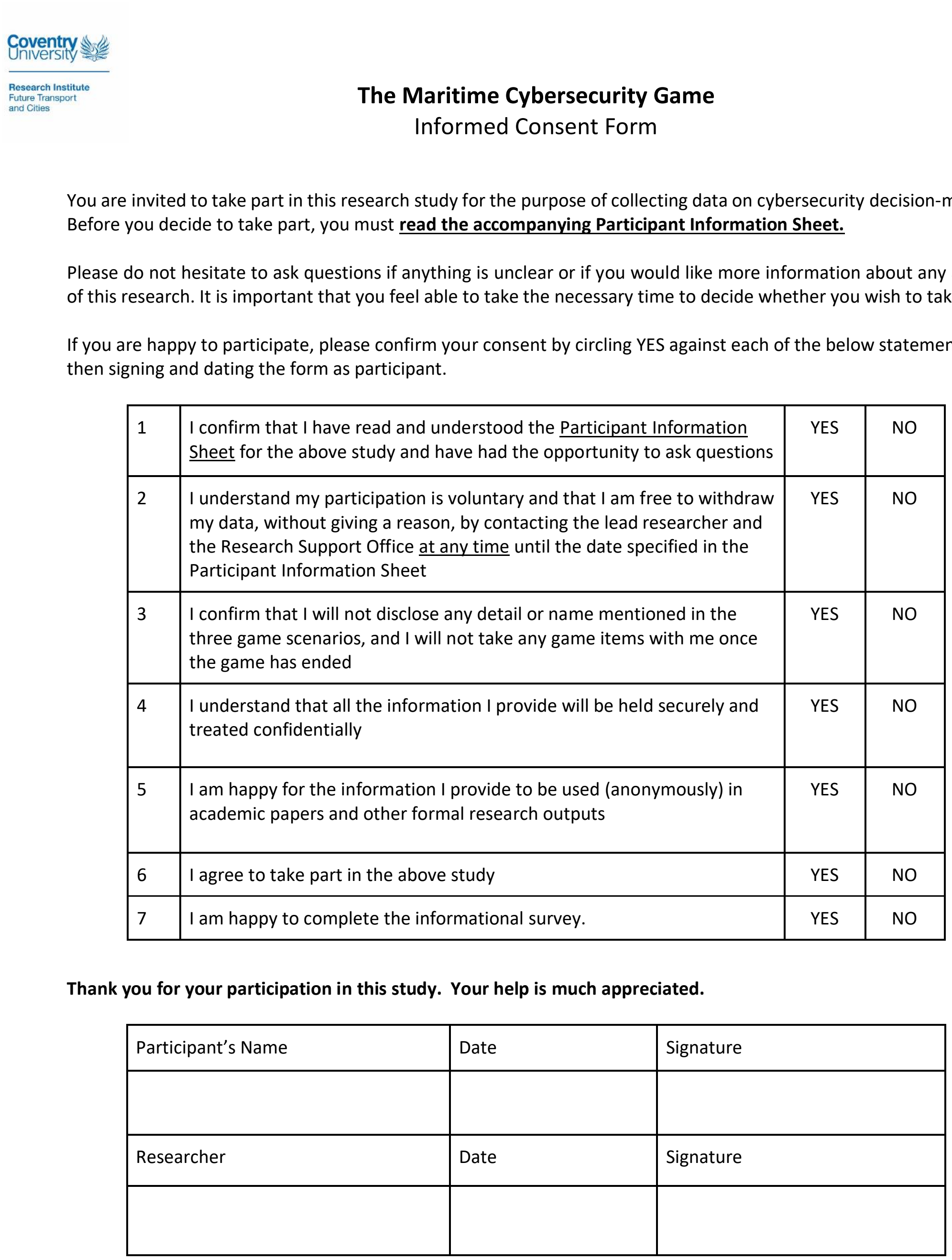
Kuhn, K., Bicakci, S. & Shaikh, S. (2020) Maritime Cyber Risk Perception and Response. In *4th NMIOTC Conference on Cybersecurity in the Maritime Domain*, pages In–Press.
https://nmiotc.nato.int/pressreleases/4th-cyber-security-conference-in-maritime-domain/.
Co-authored conference proceeding, peer-reviewed

Hussain, A., Kuhn, K. & Shaikh, S. (2020) Games for Cybersecurity Decision-making. In *Fang, X. (eds) HCI in Games. HCII 2020. Lecture Notes in Computer Science, vol 12211,* Springer.
DOI: 10.1007/978-3-030-50164-8_30.
Co-authored conference proceeding, peer-reviewed

Kuhn, K., Vasudevan, S. & Carr, M. (2020) Cyber Insurance and Risk Management: Challenges and Opportunities. *Research Institute for Sociotechnical Cyber Security.*
https://www.riscs.org.uk/cyber-insurance/.
Co-authored report

Annex B

Informed Consent Forms



Coventry University
Research Institute
Future Transport
and Cities

The Maritime Cybersecurity Game
Informed Consent Form

You are invited to take part in this research study for the purpose of collecting data on cybersecurity decision-making. Before you decide to take part, you must **read the accompanying Participant Information Sheet.**

Please do not hesitate to ask questions if anything is unclear or if you would like more information about any aspect of this research. It is important that you feel able to take the necessary time to decide whether you wish to take part.

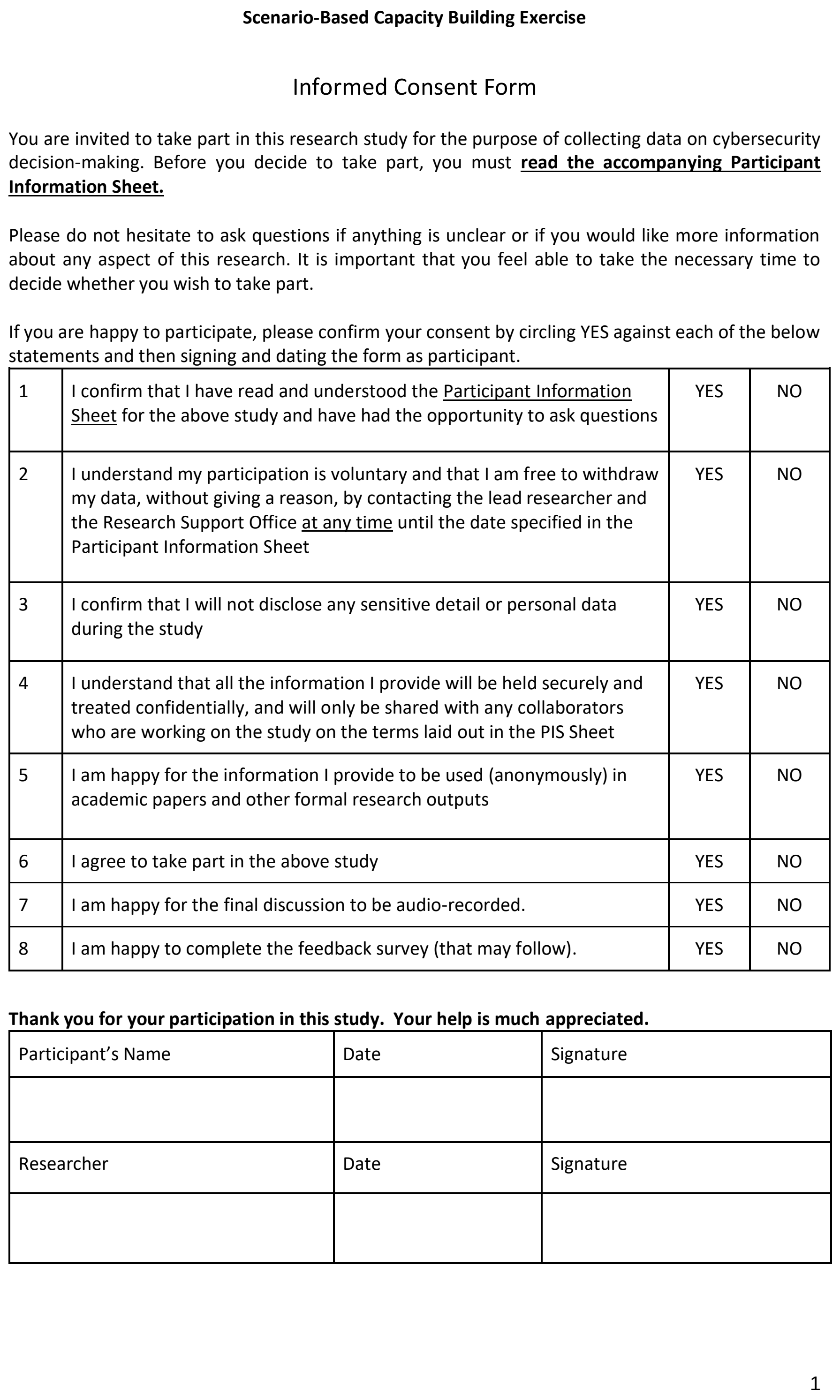
If you are happy to participate, please confirm your consent by circling YES against each of the below statements and then signing and dating the form as participant.

1	I confirm that I have read and understood the Participant Information Sheet for the above study and have had the opportunity to ask questions	YES	NO
2	I understand my participation is voluntary and that I am free to withdraw my data, without giving a reason, by contacting the lead researcher and the Research Support Office at any time until the date specified in the Participant Information Sheet	YES	NO
3	I confirm that I will not disclose any detail or name mentioned in the three game scenarios, and I will not take any game items with me once the game has ended	YES	NO
4	I understand that all the information I provide will be held securely and treated confidentially	YES	NO
5	I am happy for the information I provide to be used (anonymously) in academic papers and other formal research outputs	YES	NO
6	I agree to take part in the above study	YES	NO
7	I am happy to complete the informational survey.	YES	NO

Thank you for your participation in this study. Your help is much appreciated.

Participant's Name	Date	Signature
Researcher	Date	Signature

Exercise 1



Scenario-Based Capacity Building Exercise

Informed Consent Form

You are invited to take part in this research study for the purpose of collecting data on cybersecurity decision-making. Before you decide to take part, you must **read the accompanying Participant Information Sheet.**

Please do not hesitate to ask questions if anything is unclear or if you would like more information about any aspect of this research. It is important that you feel able to take the necessary time to decide whether you wish to take part.

If you are happy to participate, please confirm your consent by circling YES against each of the below statements and then signing and dating the form as participant.

1	I confirm that I have read and understood the Participant Information Sheet for the above study and have had the opportunity to ask questions	YES	NO
2	I understand my participation is voluntary and that I am free to withdraw my data, without giving a reason, by contacting the lead researcher and the Research Support Office at any time until the date specified in the Participant Information Sheet	YES	NO
3	I confirm that I will not disclose any sensitive detail or personal data during the study	YES	NO
4	I understand that all the information I provide will be held securely and treated confidentially, and will only be shared with any collaborators who are working on the study on the terms laid out in the PIS Sheet	YES	NO
5	I am happy for the information I provide to be used (anonymously) in academic papers and other formal research outputs	YES	NO
6	I agree to take part in the above study	YES	NO
7	I am happy for the final discussion to be audio-recorded.	YES	NO
8	I am happy to complete the feedback survey (that may follow).	YES	NO

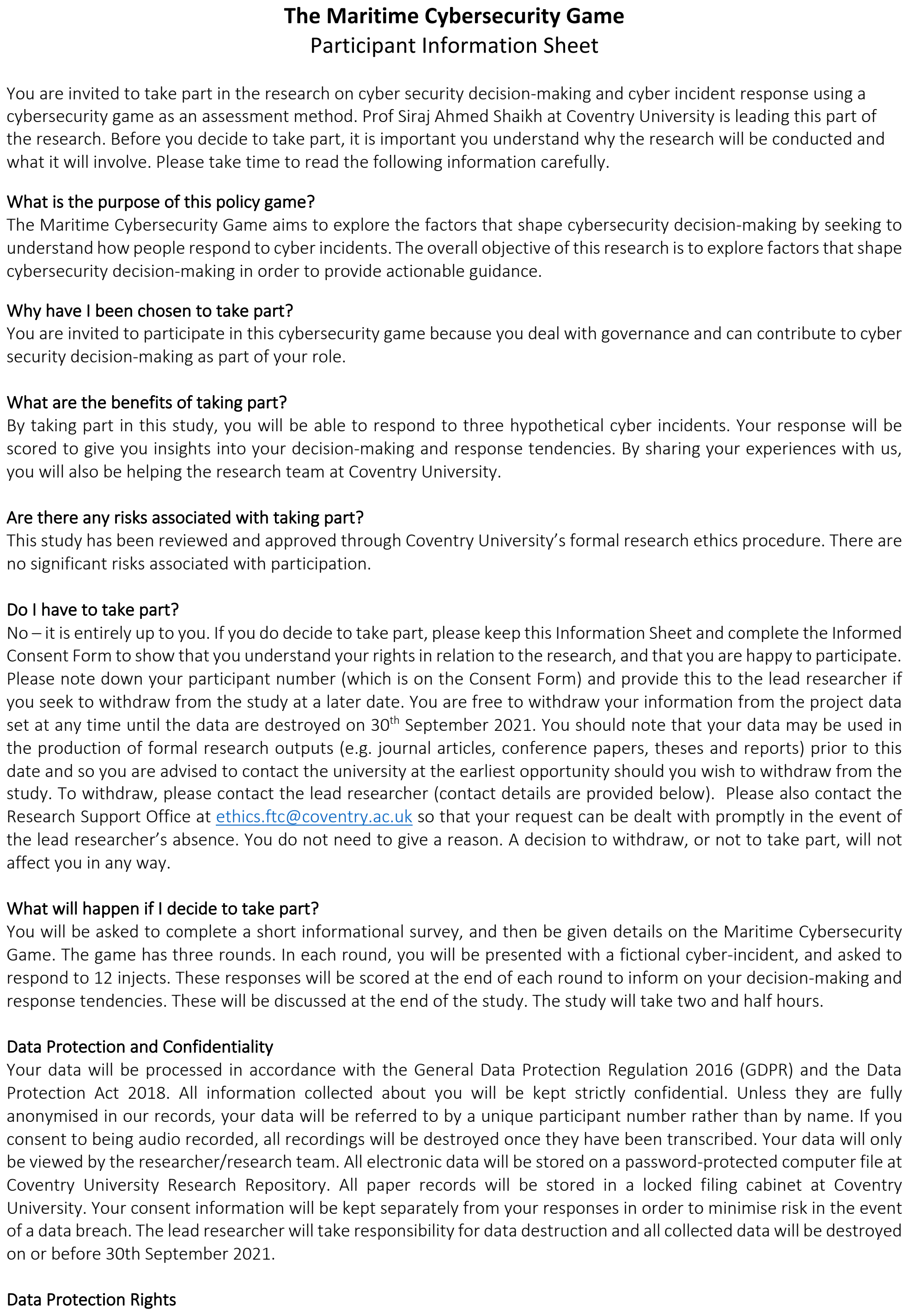
Thank you for your participation in this study. Your help is much appreciated.

Participant's Name	Date	Signature
Researcher	Date	Signature

Exercise 2

Annex C

Participant Information Sheets



The Maritime Cybersecurity Game

Participant Information Sheet

You are invited to take part in the research on cyber security decision-making and cyber incident response using a cybersecurity game as an assessment method. Prof Siraj Ahmed Shaikh at Coventry University is leading this part of the research. Before you decide to take part, it is important you understand why the research will be conducted and what it will involve. Please take time to read the following information carefully.

What is the purpose of this policy game?

The Maritime Cybersecurity Game aims to explore the factors that shape cybersecurity decision-making by seeking to understand how people respond to cyber incidents. The overall objective of this research is to explore factors that shape cybersecurity decision-making in order to provide actionable guidance.

Why have I been chosen to take part?

You are invited to participate in this cybersecurity game because you deal with governance and can contribute to cyber security decision-making as part of your role.

What are the benefits of taking part?

By taking part in this study, you will be able to respond to three hypothetical cyber incidents. Your response will be scored to give you insights into your decision-making and response tendencies. By sharing your experiences with us, you will also be helping the research team at Coventry University.

Are there any risks associated with taking part?

This study has been reviewed and approved through Coventry University's formal research ethics procedure. There are no significant risks associated with participation.

Do I have to take part?

No – it is entirely up to you. If you do decide to take part, please keep this Information Sheet and complete the Informed Consent Form to show that you understand your rights in relation to the research, and that you are happy to participate. Please note down your participant number (which is on the Consent Form) and provide this to the lead researcher if you seek to withdraw from the study at a later date. You are free to withdraw your information from the project data set at any time until the data are destroyed on 30th September 2021. You should note that your data may be used in the production of formal research outputs (e.g. journal articles, conference papers, theses and reports) prior to this date and so you are advised to contact the university at the earliest opportunity should you wish to withdraw from the study. To withdraw, please contact the lead researcher (contact details are provided below). Please also contact the Research Support Office at ethics.ftc@coventry.ac.uk so that your request can be dealt with promptly in the event of the lead researcher's absence. You do not need to give a reason. A decision to withdraw, or not to take part, will not affect you in any way.

What will happen if I decide to take part?

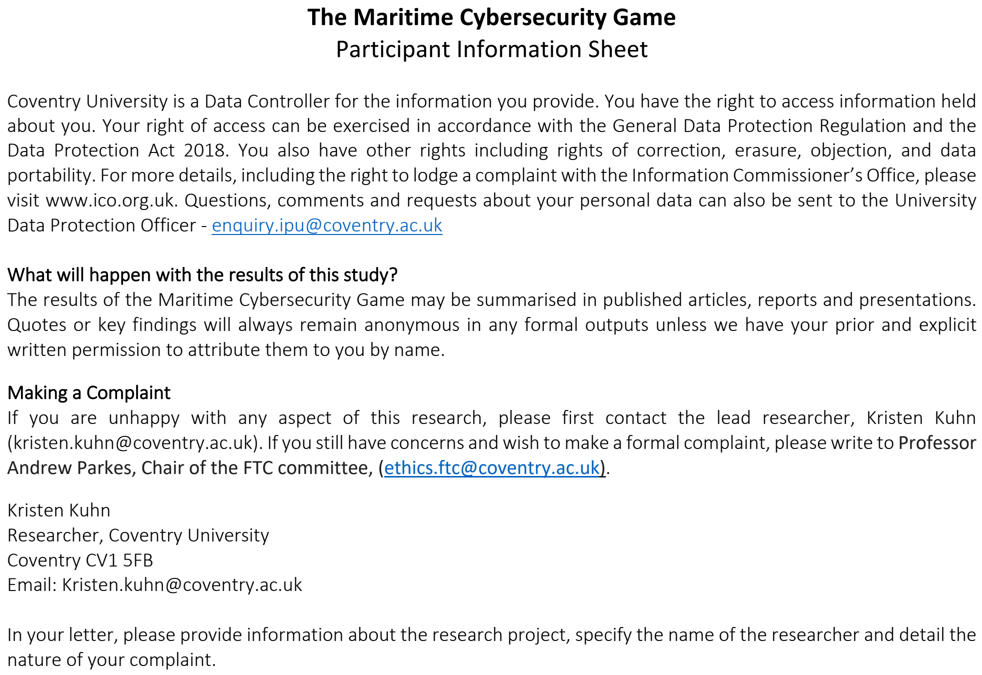
You will be asked to complete a short informational survey, and then be given details on the Maritime Cybersecurity Game. The game has three rounds. In each round, you will be presented with a fictional cyber-incident, and asked to respond to 12 injects. These responses will be scored at the end of each round to inform on your decision-making and response tendencies. These will be discussed at the end of the study. The study will take two and half hours.

Data Protection and Confidentiality

Your data will be processed in accordance with the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018. All information collected about you will be kept strictly confidential. Unless they are fully anonymised in our records, your data will be referred to by a unique participant number rather than by name. If you consent to being audio recorded, all recordings will be destroyed once they have been transcribed. Your data will only be viewed by the researcher/research team. All electronic data will be stored on a password-protected computer file at Coventry University Research Repository. All paper records will be stored in a locked filing cabinet at Coventry University. Your consent information will be kept separately from your responses in order to minimise risk in the event of a data breach. The lead researcher will take responsibility for data destruction and all collected data will be destroyed on or before 30th September 2021.

Data Protection Rights

Exercise 1



The Maritime Cybersecurity Game

Participant Information Sheet

Coventry University is a Data Controller for the information you provide. You have the right to access information held about you. Your right of access can be exercised in accordance with the General Data Protection Regulation and the Data Protection Act 2018. You also have other rights including rights of correction, erasure, objection, and data portability. For more details, including the right to lodge a complaint with the Information Commissioner's Office, please visit www.ico.org.uk. Questions, comments and requests about your personal data can also be sent to the University Data Protection Officer - enquiry.ipu@coventry.ac.uk

What will happen with the results of this study?

The results of the Maritime Cybersecurity Game may be summarised in published articles, reports and presentations. Quotes or key findings will always remain anonymous in any formal outputs unless we have your prior and explicit written permission to attribute them to you by name.

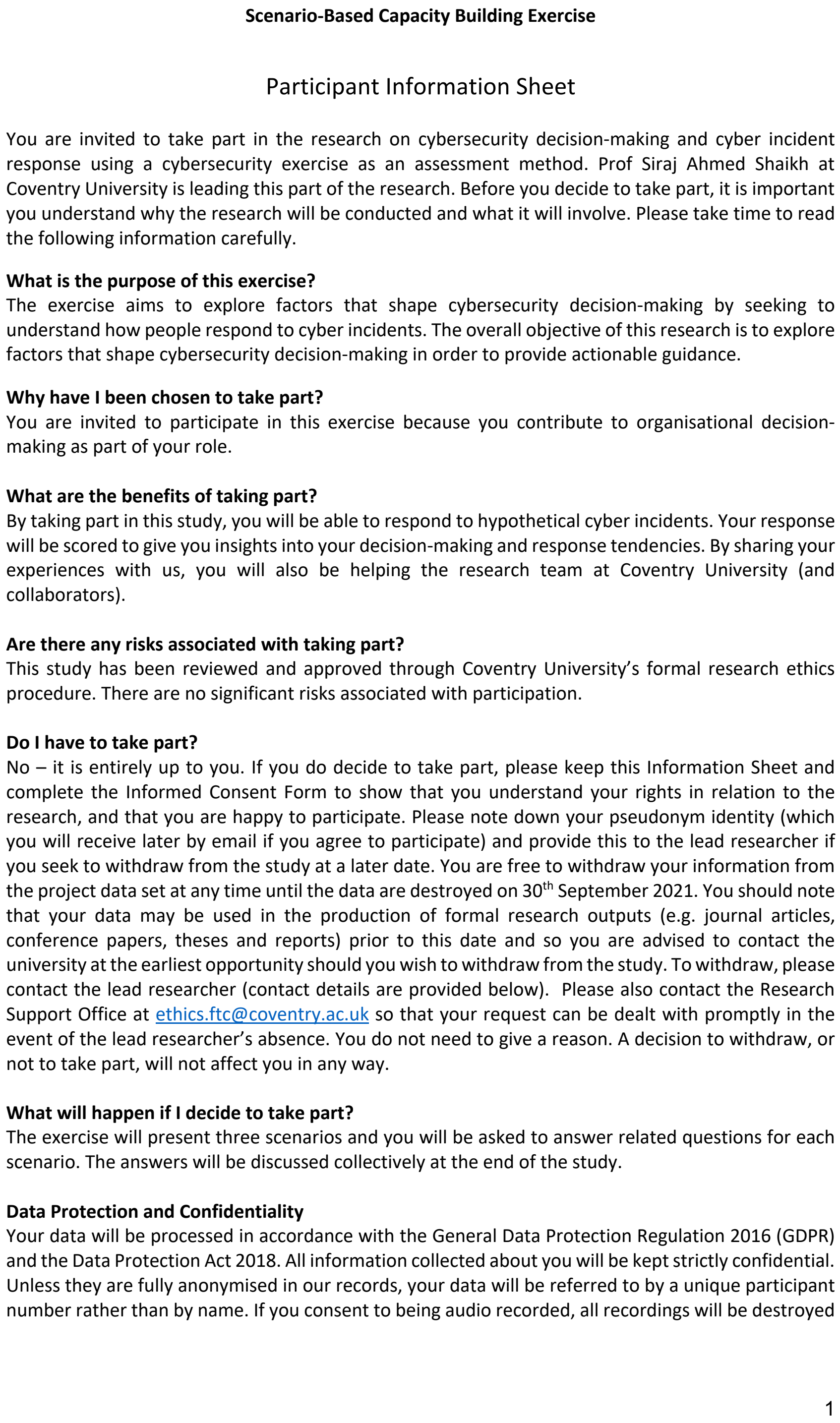
Making a Complaint

If you are unhappy with any aspect of this research, please first contact the lead researcher, Kristen Kuhn (kristen.kuhn@coventry.ac.uk). If you still have concerns and wish to make a formal complaint, please write to Professor Andrew Parkes, Chair of the FTC committee, (ethics.ftc@coventry.ac.uk).

Kristen Kuhn
Researcher, Coventry University
Coventry CV1 5FB
Email: Kristen.kuhn@coventry.ac.uk

In your letter, please provide information about the research project, specify the name of the researcher and detail the nature of your complaint.

Exercise 1



Scenario-Based Capacity Building Exercise

Participant Information Sheet

You are invited to take part in the research on cybersecurity decision-making and cyber incident response using a cybersecurity exercise as an assessment method. Prof Siraj Ahmed Shaikh at Coventry University is leading this part of the research. Before you decide to take part, it is important you understand why the research will be conducted and what it will involve. Please take time to read the following information carefully.

What is the purpose of this exercise?
The exercise aims to explore factors that shape cybersecurity decision-making by seeking to understand how people respond to cyber incidents. The overall objective of this research is to explore factors that shape cybersecurity decision-making in order to provide actionable guidance.

Why have I been chosen to take part?
You are invited to participate in this exercise because you contribute to organisational decision-making as part of your role.

What are the benefits of taking part?
By taking part in this study, you will be able to respond to hypothetical cyber incidents. Your response will be scored to give you insights into your decision-making and response tendencies. By sharing your experiences with us, you will also be helping the research team at Coventry University (and collaborators).

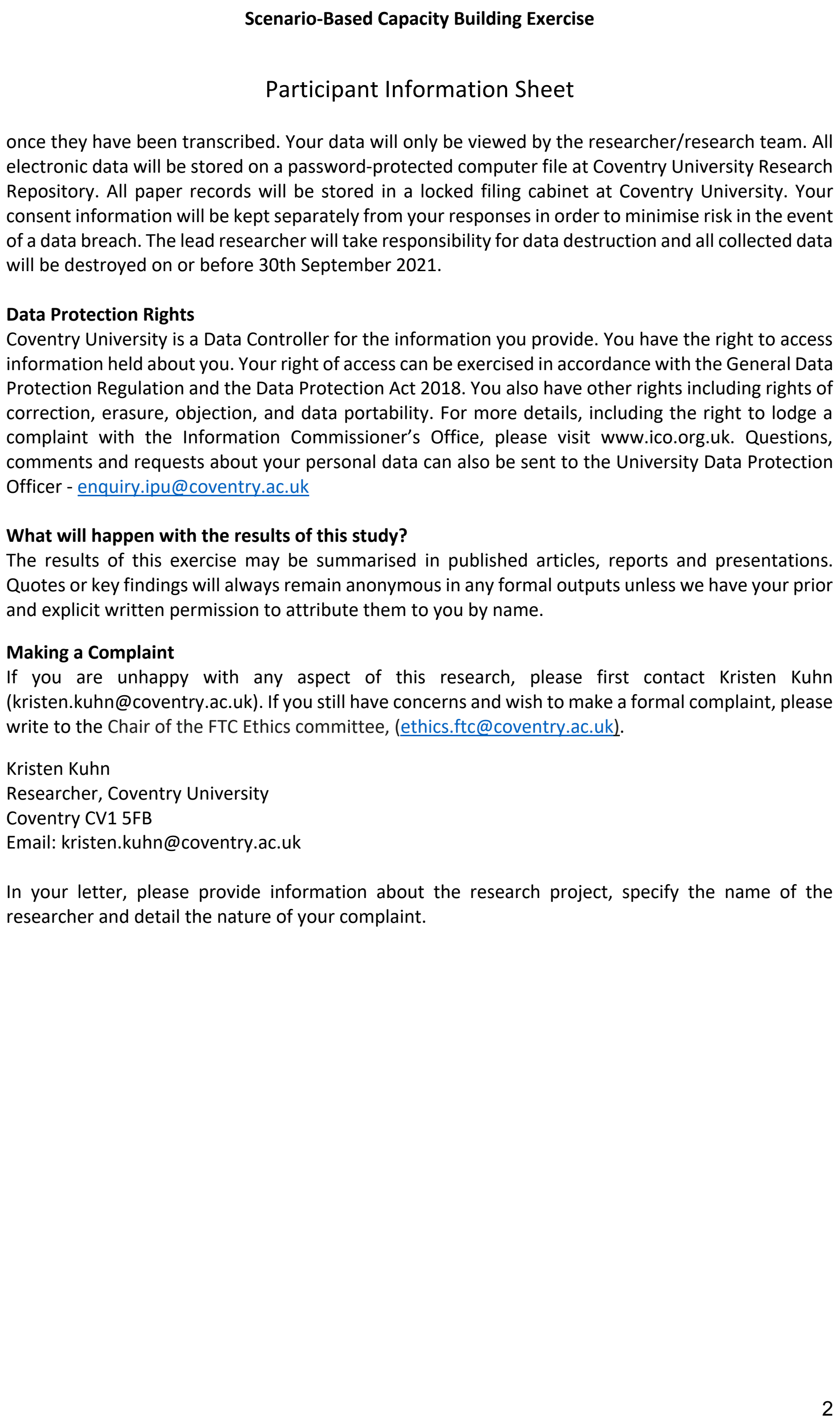
Are there any risks associated with taking part?
This study has been reviewed and approved through Coventry University's formal research ethics procedure. There are no significant risks associated with participation.

Do I have to take part?
No – it is entirely up to you. If you do decide to take part, please keep this Information Sheet and complete the Informed Consent Form to show that you understand your rights in relation to the research, and that you are happy to participate. Please note down your pseudonym identity (which you will receive later by email if you agree to participate) and provide this to the lead researcher if you seek to withdraw from the study at a later date. You are free to withdraw your information from the project data set at any time until the data are destroyed on 30th September 2021. You should note that your data may be used in the production of formal research outputs (e.g. journal articles, conference papers, theses and reports) prior to this date and so you are advised to contact the university at the earliest opportunity should you wish to withdraw from the study. To withdraw, please contact the lead researcher (contact details are provided below). Please also contact the Research Support Office at ethics.ftc@coventry.ac.uk so that your request can be dealt with promptly in the event of the lead researcher's absence. You do not need to give a reason. A decision to withdraw, or not to take part, will not affect you in any way.

What will happen if I decide to take part?
The exercise will present three scenarios and you will be asked to answer related questions for each scenario. The answers will be discussed collectively at the end of the study.

Data Protection and Confidentiality
Your data will be processed in accordance with the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018. All information collected about you will be kept strictly confidential. Unless they are fully anonymised in our records, your data will be referred to by a unique participant number rather than by name. If you consent to being audio recorded, all recordings will be destroyed

Exercise 2



Scenario-Based Capacity Building Exercise

Participant Information Sheet

once they have been transcribed. Your data will only be viewed by the researcher/research team. All electronic data will be stored on a password-protected computer file at Coventry University Research Repository. All paper records will be stored in a locked filing cabinet at Coventry University. Your consent information will be kept separately from your responses in order to minimise risk in the event of a data breach. The lead researcher will take responsibility for data destruction and all collected data will be destroyed on or before 30th September 2021.

Data Protection Rights

Coventry University is a Data Controller for the information you provide. You have the right to access information held about you. Your right of access can be exercised in accordance with the General Data Protection Regulation and the Data Protection Act 2018. You also have other rights including rights of correction, erasure, objection, and data portability. For more details, including the right to lodge a complaint with the Information Commissioner's Office, please visit www.ico.org.uk. Questions, comments and requests about your personal data can also be sent to the University Data Protection Officer - enquiry.ipu@coventry.ac.uk

What will happen with the results of this study?

The results of this exercise may be summarised in published articles, reports and presentations. Quotes or key findings will always remain anonymous in any formal outputs unless we have your prior and explicit written permission to attribute them to you by name.

Making a Complaint

If you are unhappy with any aspect of this research, please first contact Kristen Kuhn (kristen.kuhn@coventry.ac.uk). If you still have concerns and wish to make a formal complaint, please write to the Chair of the FTC Ethics committee, (ethics.ftc@coventry.ac.uk).

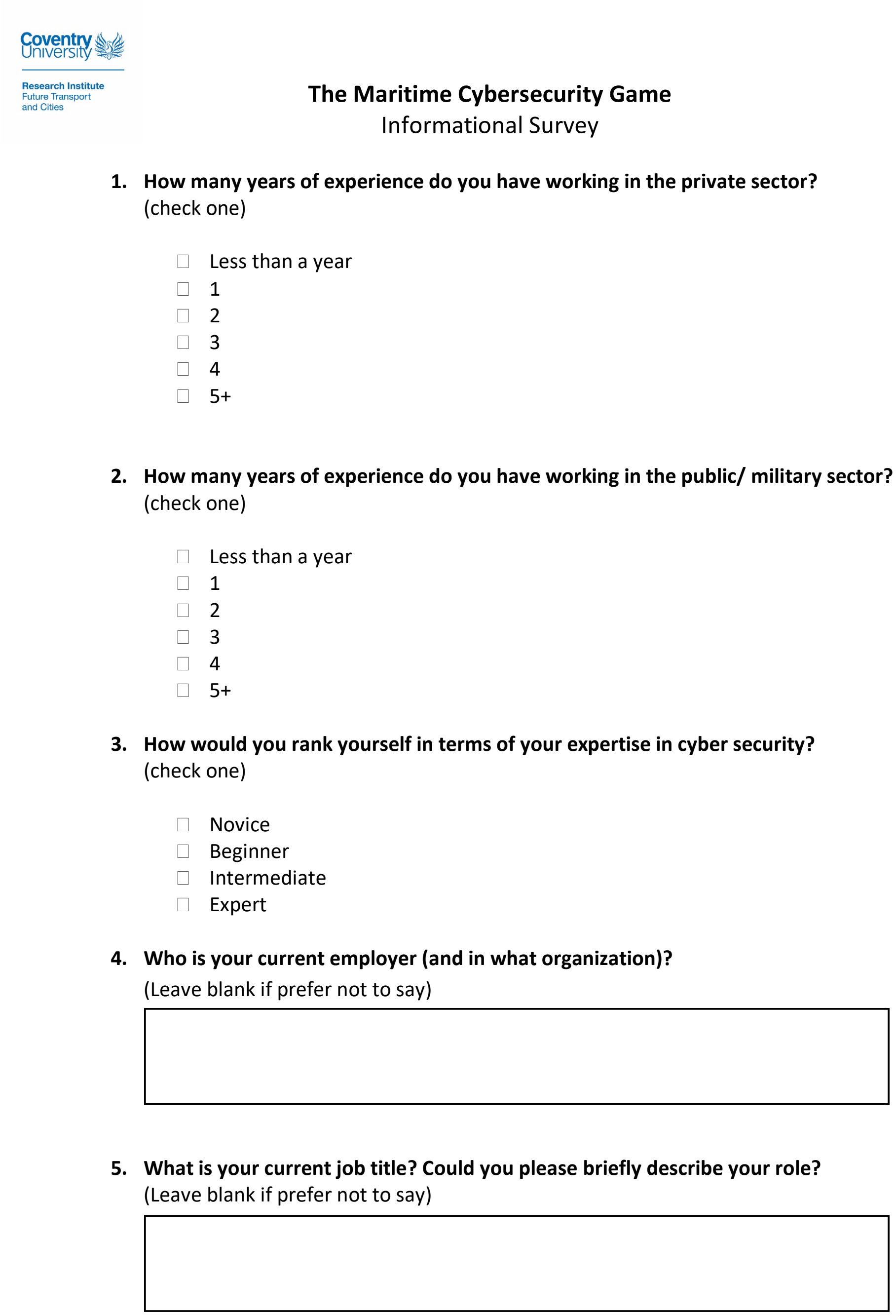
Kristen Kuhn
Researcher, Coventry University
Coventry CV1 5FB
Email: kristen.kuhn@coventry.ac.uk

In your letter, please provide information about the research project, specify the name of the researcher and detail the nature of your complaint.

Exercise 2

Annex D

Pre-exercise Questionnaires



The Maritime Cybersecurity Game

Informational Survey

1. **How many years of experience do you have working in the private sector?**
   (check one)

   □ Less than a year
   □ 1
   □ 2
   □ 3
   □ 4
   □ 5+

2. **How many years of experience do you have working in the public/ military sector?**
   (check one)

   □ Less than a year
   □ 1
   □ 2
   □ 3
   □ 4
   □ 5+

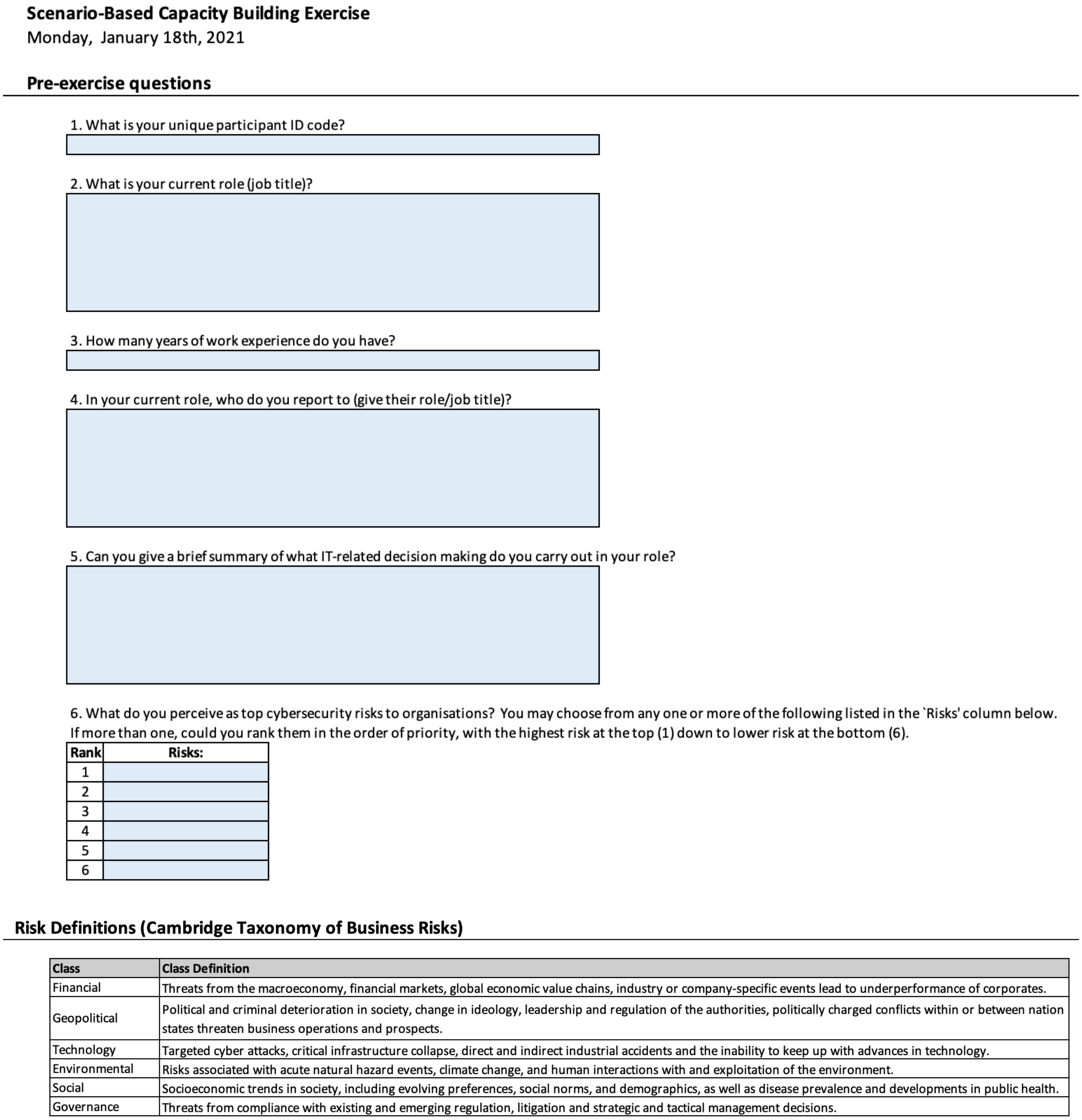
3. **How would you rank yourself in terms of your expertise in cyber security?**
   (check one)

   □ Novice
   □ Beginner
   □ Intermediate
   □ Expert

4. **Who is your current employer (and in what organization)?**
   (Leave blank if prefer not to say)

5. **What is your current job title? Could you please briefly describe your role?**
   (Leave blank if prefer not to say)

Exercise 1



Scenario-Based Capacity Building Exercise

Monday, January 18th, 2021

Pre-exercise questions

1. What is your unique participant ID code?

2. What is your current role (job title)?

3. How many years of work experience do you have?

4. In your current role, who do you report to (give their role/job title)?

5. Can you give a brief summary of what IT-related decision making do you carry out in your role?

6. What do you perceive as top cybersecurity risks to organisations? You may choose from any one or more of the following listed in the `Risks' column below. If more than one, could you rank them in the order of priority, with the highest risk at the top (1) down to lower risk at the bottom (6).

Rank	Risks:
1	
2	
3	
4	
5	
6	

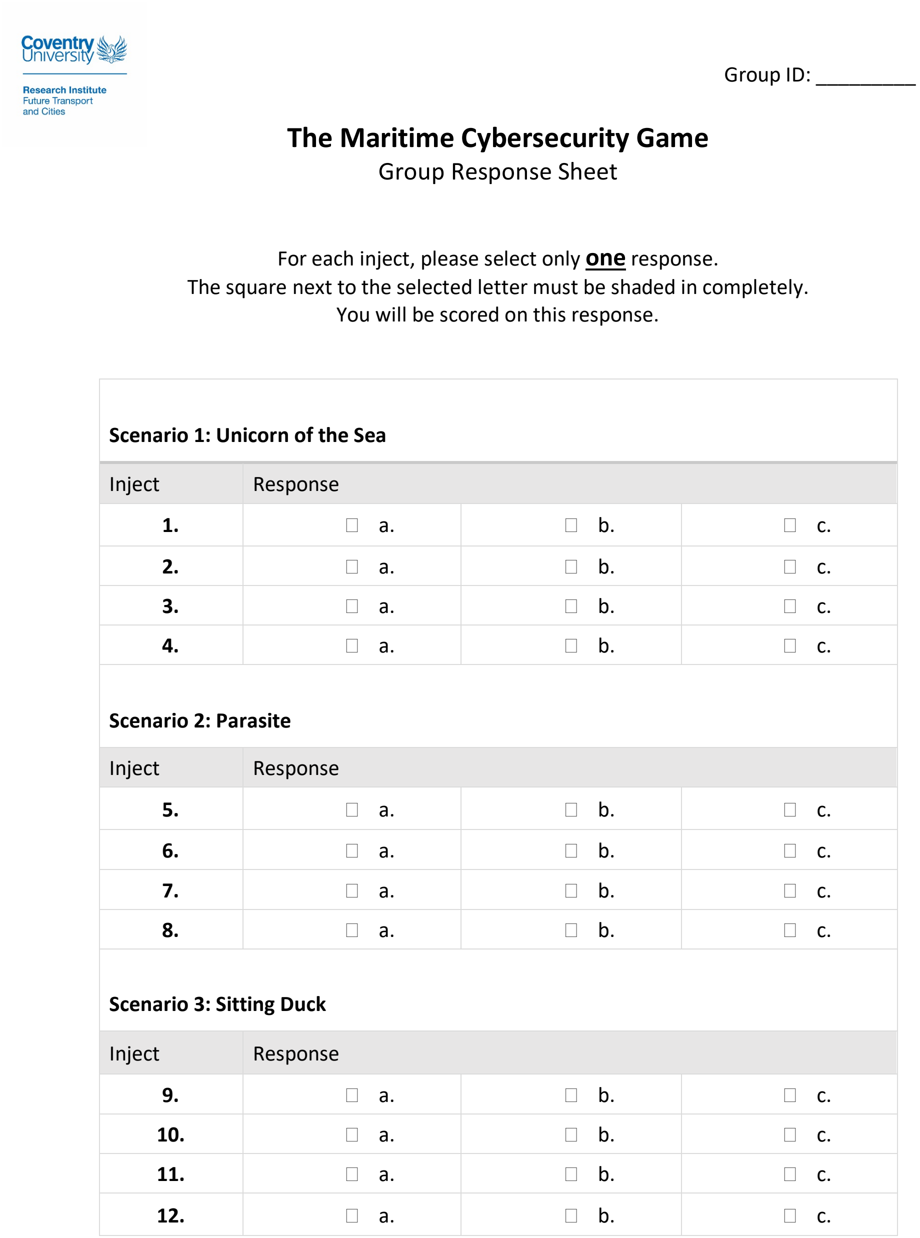
Risk Definitions (Cambridge Taxonomy of Business Risks)

Class	Class Definition
Financial	Threats from the macroeconomy, financial markets, global economic value chains, industry or company-specific events lead to underperformance of corporates.
Geopolitical	Political and criminal deterioration in society, change in ideology, leadership and regulation of the authorities, politically charged conflicts within or between nation states threaten business operations and prospects.
Technology	Targeted cyber attacks, critical infrastructure collapse, direct and indirect industrial accidents and the inability to keep up with advances in technology.
Environmental	Risks associated with acute natural hazard events, climate change, and human interactions with and exploitation of the environment.
Social	Socioeconomic trends in society, including evolving preferences, social norms, and demographics, as well as disease prevalence and developments in public health.
Governance	Threats from compliance with existing and emerging regulation, litigation and strategic and tactical management decisions.

Exercise 2

Annex E

Scenario Questions



Coventry University
Research Institute
Future Transport
and Cities

Group ID: _________

The Maritime Cybersecurity Game

Group Response Sheet

For each inject, please select only **one** response.
The square next to the selected letter must be shaded in completely.
You will be scored on this response.

Scenario 1: Unicorn of the Sea

Inject	Response		
1.	□ a.	□ b.	□ c.
2.	□ a.	□ b.	□ c.
3.	□ a.	□ b.	□ c.
4.	□ a.	□ b.	□ c.

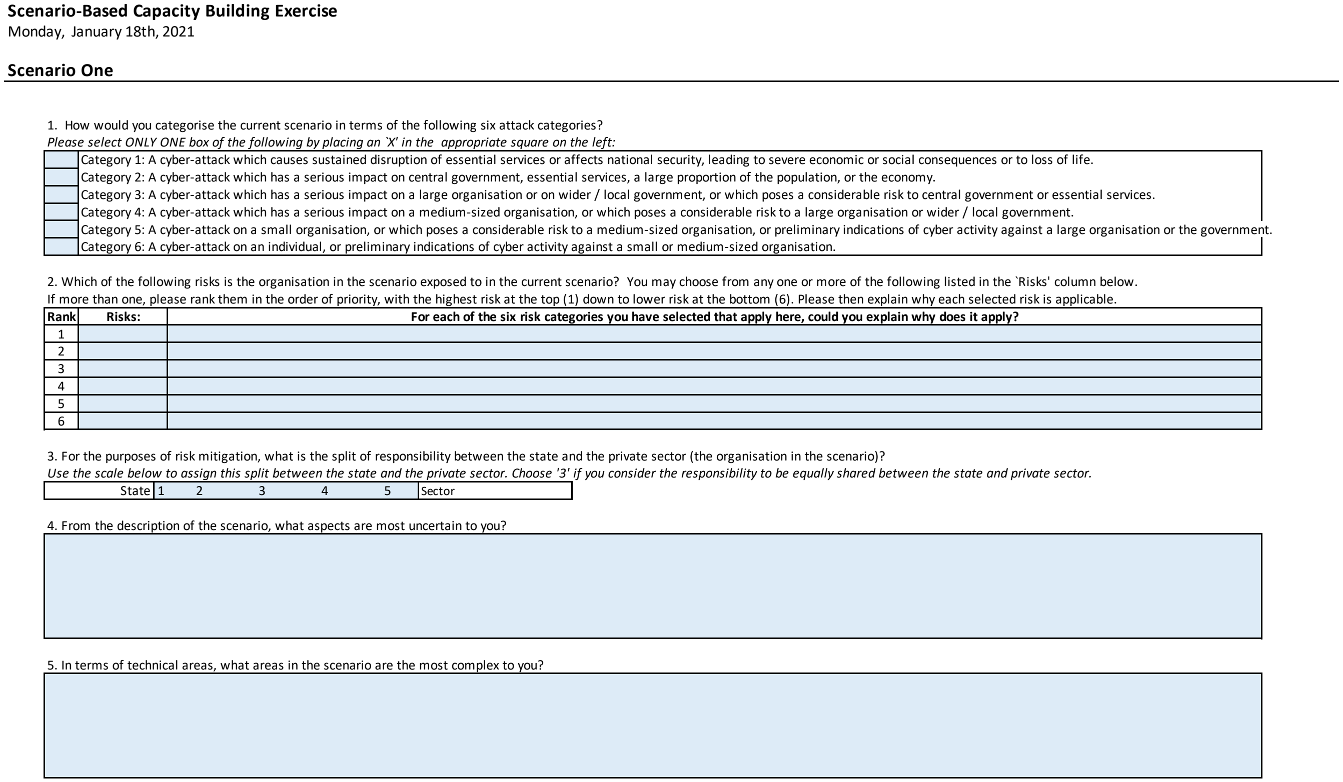
Scenario 2: Parasite

Inject	Response		
5.	□ a.	□ b.	□ c.
6.	□ a.	□ b.	□ c.
7.	□ a.	□ b.	□ c.
8.	□ a.	□ b.	□ c.

Scenario 3: Sitting Duck

Inject	Response		
9.	□ a.	□ b.	□ c.
10.	□ a.	□ b.	□ c.
11.	□ a.	□ b.	□ c.
12.	□ a.	□ b.	□ c.

Exercise 1



Scenario-Based Capacity Building Exercise
Monday, January 18th, 2021

Scenario One

1. How would you categorise the current scenario in terms of the following six attack categories?
Please select ONLY ONE box of the following by placing an 'X' in the appropriate square on the left:

□	Category 1: A cyber-attack which causes sustained disruption of essential services or affects national security, leading to severe economic or social consequences or to loss of life.
□	Category 2: A cyber-attack which has a serious impact on central government, essential services, a large proportion of the population, or the economy.
□	Category 3: A cyber-attack which has a serious impact on a large organisation or on wider / local government, or which poses a considerable risk to central government or essential services.
□	Category 4: A cyber-attack which has a serious impact on a medium-sized organisation, or which poses a considerable risk to a large organisation or wider / local government.
□	Category 5: A cyber-attack on a small organisation, or which poses a considerable risk to a medium-sized organisation, or preliminary indications of cyber activity against a large organisation or the government.
□	Category 6: A cyber-attack on an individual, or preliminary indications of cyber activity against a small or medium-sized organisation.

2. Which of the following risks is the organisation in the scenario exposed to in the current scenario? You may choose from any one or more of the following listed in the `Risks' column below.
If more than one, please rank them in the order of priority, with the highest risk at the top (1) down to lower risk at the bottom (6). Please then explain why each selected risk is applicable.

Rank	Risks:	For each of the six risk categories you have selected that apply here, could you explain why does it apply?
1		
2		
3		
4		
5		
6		

3. For the purposes of risk mitigation, what is the split of responsibility between the state and the private sector (the organisation in the scenario)?
Use the scale below to assign this split between the state and the private sector. Choose '3' if you consider the responsibility to be equally shared between the state and private sector.

State	1	2	3	4	5	Sector

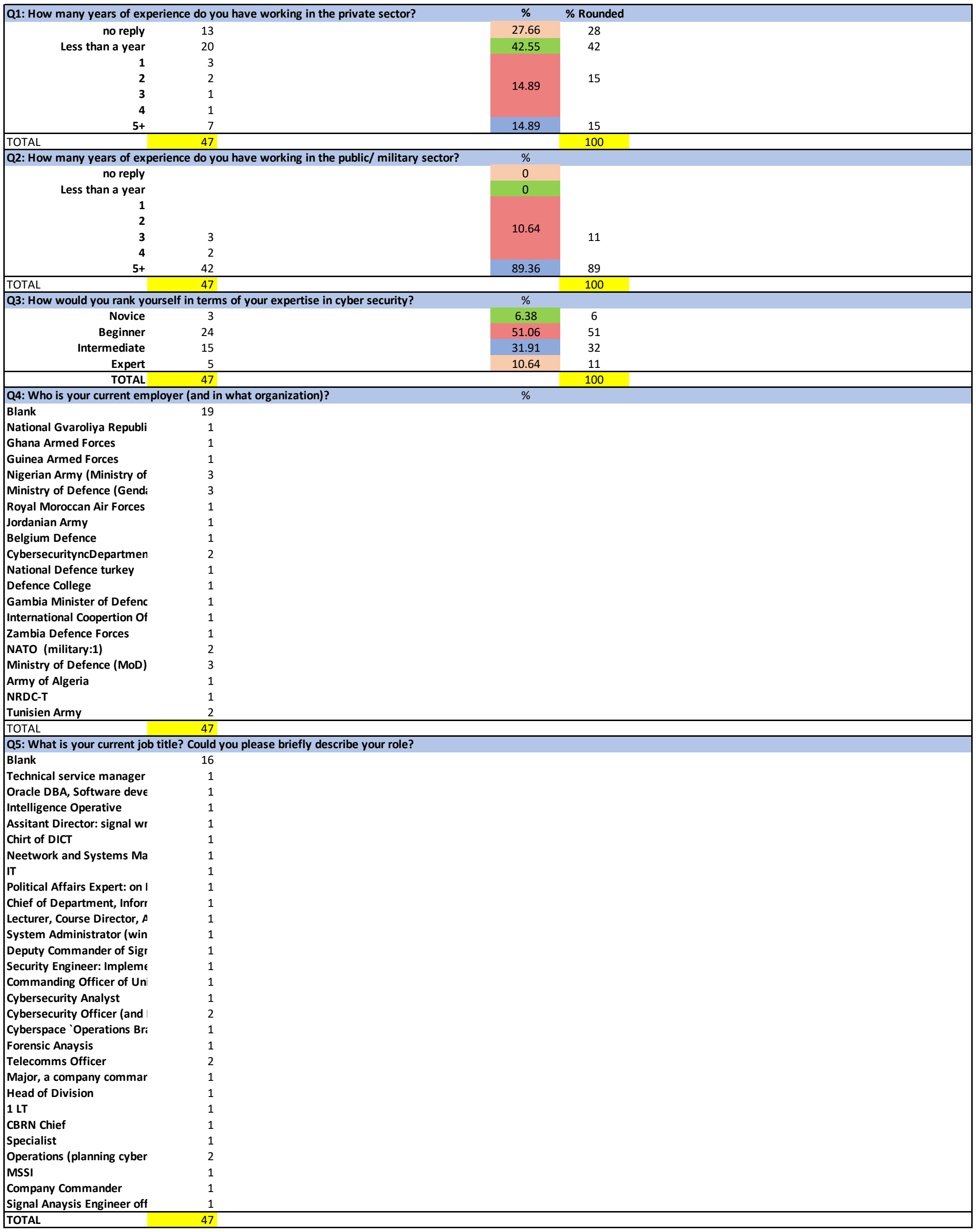
4. From the description of the scenario, what aspects are most uncertain to you?

5. In terms of technical areas, what areas in the scenario are the most complex to you?

Exercise 2

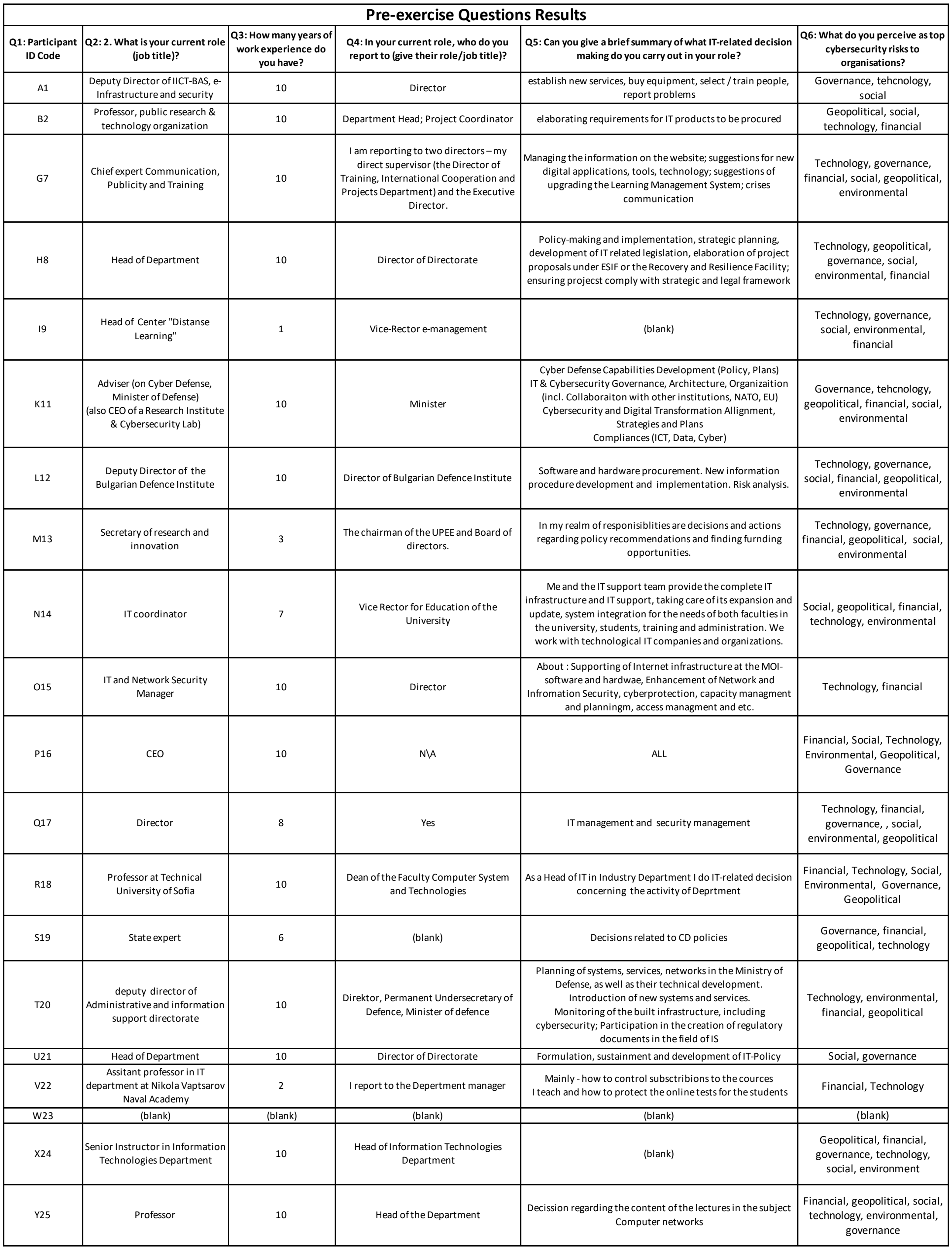
Annex F

Pre-exercise Questions Results



Q1: How many years of experience do you have working in the private sector?		%	% Rounded
no reply	13	27.66	28
Less than a year	20	42.55	42
1	3	14.89	
2	2		15
3	1		
4	1		
5+	7	14.89	15
TOTAL	47		100
Q2: How many years of experience do you have working in the public/ military sector?		%	
no reply		0	
Less than a year		0	
1		10.64	
2			
3	3		11
4	2		
5+	42	89.36	89
TOTAL	47		100
Q3: How would you rank yourself in terms of your expertise in cyber security?		%	
Novice	3	6.38	6
Beginner	24	51.06	51
Intermediate	15	31.91	32
Expert	5	10.64	11
TOTAL	47		100
Q4: Who is your current employer (and in what organization)?		%	
Blank	19		
National Gvaroliya Republi	1		
Ghana Armed Forces	1		
Guinea Armed Forces	1		
Nigerian Army (Ministry of	3		
Ministry of Defence (Genda	3		
Royal Moroccan Air Forces	1		
Jordanian Army	1		
Belgium Defence	1		
CybersecurityncDepartmen	2		
National Defence turkey	1		
Defence College	1		
Gambia Minister of Defenc	1		
International Coopertion Of	1		
Zambia Defence Forces	1		
NATO (military:1)	2		
Ministry of Defence (MoD)	3		
Army of Algeria	1		
NRDC-T	1		
Tunisien Army	2		
TOTAL	47		
Q5: What is your current job title? Could you please briefly describe your role?			
Blank	16		
Technical service manager	1		
Oracle DBA, Software deve	1		
Intelligence Operative	1		
Assitant Director: signal wr	1		
Chirt of DICT	1		
Neetwork and Systems Ma	1		
IT	1		
Political Affairs Expert: on	1		
Chief of Department, Inforr	1		
Lecturer, Course Director, A	1		
System Administrator (win	1		
Deputy Commander of Sigr	1		
Security Engineer: Impleme	1		
Commanding Officer of Uni	1		
Cybersecurity Analyst	1		
Cybersecurity Officer (and	2		
Cyberspace `Operations Bra	1		
Forensic Anaysis	1		
Telecomms Officer	2		
Major, a company commar	1		
Head of Division	1		
1 LT	1		
CBRN Chief	1		
Specialist	1		
Operations (planning cyber	2		
MSSI	1		
Company Commander	1		
Signal Anaysis Engineer off	1		
TOTAL	47		

Exercise 1



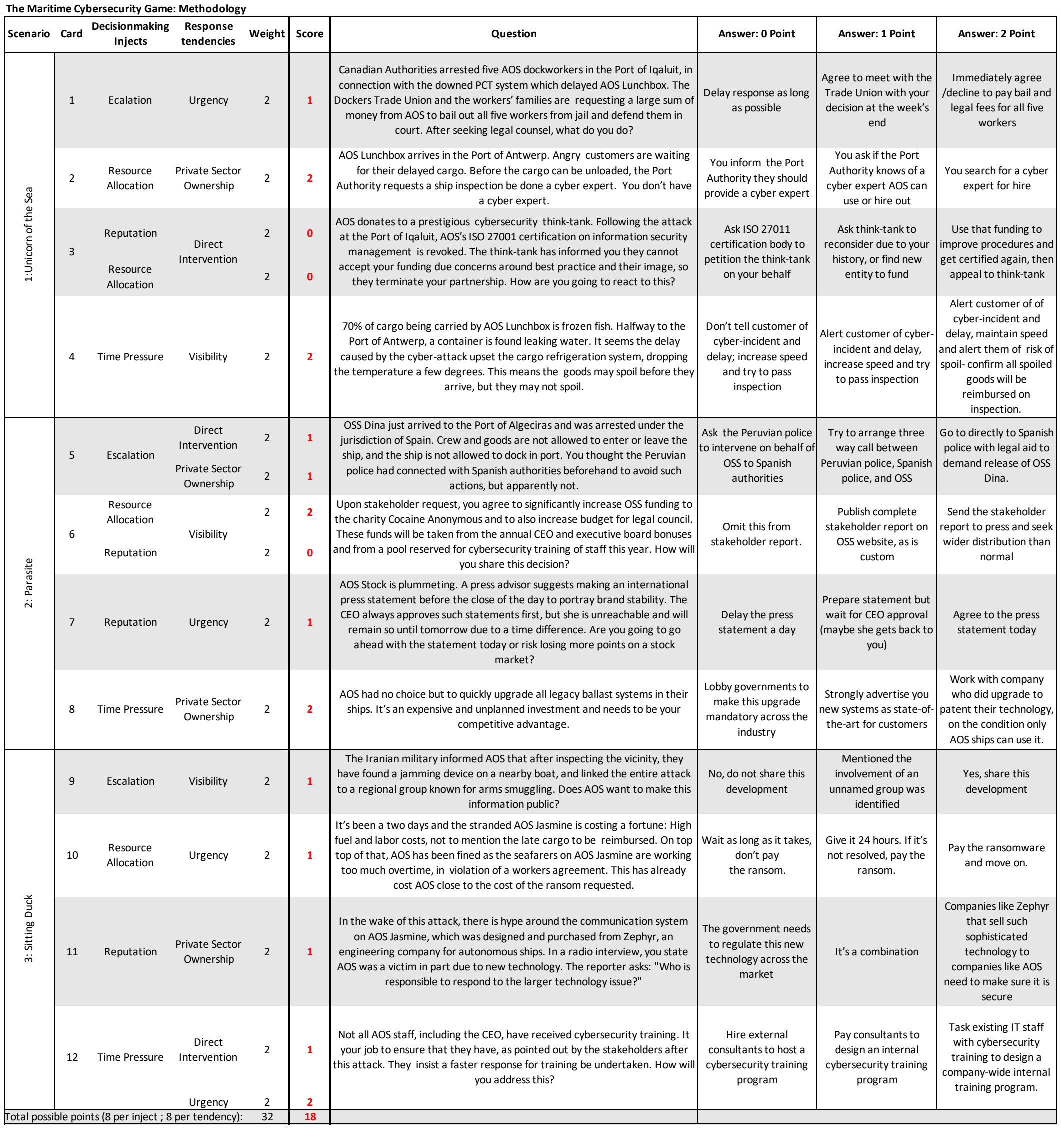
Pre-exercise Questions Results

Q1: Participant ID Code	Q2: 2. What is your current role (job title)?	Q3: How many years of work experience do you have?	Q4: In your current role, who do you report to (give their role/job title)?	Q5: Can you give a brief summary of what IT-related decision making do you carry out in your role?	Q6: What do you perceive as top cybersecurity risks to organisations?
A1	Deputy Director of IICT-BAS, e-Infrastructure and security	10	Director	establish new services, buy equipment, select / train people, report problems	Governance, tehcnology, social
B2	Professor, public research & technology organization	10	Department Head; Project Coordinator	elaborating requirements for IT products to be procured	Geopolitical, social, technology, financial
G7	Chief expert Communication, Publicity and Training	10	I am reporting to two directors – my direct supervisor (the Director of Training, International Cooperation and Projects Department) and the Executive Director.	Managing the information on the website; suggestions for new digital applications, tools, technology; suggestions of upgrading the Learning Management System; crises communication	Technology, governance, financial, social, geopolitical, environmental
H8	Head of Department	10	Director of Directorate	Policy-making and implementation, strategic planning, development of IT related legislation, elaboration of project proposals under ESIF or the Recovery and Resilience Facility; ensuring projecst comply with strategic and legal framework	Technology, geopolitical, governance, social, environmental, financial
I9	Head of Center "Distanse Learning"	1	Vice-Rector e-management	(blank)	Technology, governance, social, environmental, financial
K11	Adviser (on Cyber Defense, Minister of Defense) (also CEO of a Research Institute & Cybersecurity Lab)	10	Minister	Cyber Defense Capabilities Development (Policy, Plans) IT & Cybersecurity Governance, Architecture, Organizaition (incl. Collaboraiton with other institutions, NATO, EU) Cybersecurity and Digital Transformation Allignment, Strategies and Plans Compliances (ICT, Data, Cyber)	Governance, tehcnology, geopolitical, financial, social, environmental
L12	Deputy Director of the Bulgarian Defence Institute	10	Director of Bulgarian Defence Institute	Software and hardware procurement. New information procedure development and implementation. Risk analysis.	Technology, governance, social, financial, geopolitical, environmental
M13	Secretary of research and innovation	3	The chairman of the UPEE and Board of directors.	In my realm of responisiblities are decisions and actions regarding policy recommendations and finding furnding opportunities.	Technology, governance, financial, geopolitical, social, environmental
N14	IT coordinator	7	Vice Rector for Education of the University	Me and the IT support team provide the complete IT infrastructure and IT support, taking care of its expansion and update, system integration for the needs of both faculties in the university, students, training and administration. We work with technological IT companies and organizations.	Social, geopolitical, financial, technology, environmental
O15	IT and Network Security Manager	10	Director	About : Supporting of Internet infrastructure at the MOI-software and hardwae, Enhancement of Network and Infromation Security, cyberprotection, capacity managment and planningm, access managment and etc.	Technology, financial
P16	CEO	10	N\A	ALL	Financial, Social, Technology, Environmental, Geopolitical, Governance
Q17	Director	8	Yes	IT management and security management	Technology, financial, governance, , social, environmental, geopolitical
R18	Professor at Technical University of Sofia	10	Dean of the Faculty Computer System and Technologies	As a Head of IT in Industry Department I do IT-related decision concerning the activity of Deprtment	Financial, Technology, Social, Environmental, Governance, Geopolitical
S19	State expert	6	(blank)	Decisions related to CD policies	Governance, financial, geopolitical, technology
T20	deputy director of Administrative and information support directorate	10	Direktor, Permanent Undersecretary of Defence, Minister of defence	Planning of systems, services, networks in the Ministry of Defense, as well as their technical development. Introduction of new systems and services. Monitoring of the built infrastructure, including cybersecurity; Participation in the creation of regulatory documents in the field of IS	Technology, environmental, financial, geopolitical
U21	Head of Department	10	Director of Directorate	Formulation, sustainment and development of IT-Policy	Social, governance
V22	Assitant professor in IT department at Nikola Vaptsarov Naval Academy	2	I report to the Depertment manager	Mainly - how to control subsctribions to the cources I teach and how to protect the online tests for the students	Financial, Technology
W23	(blank)	(blank)	(blank)	(blank)	(blank)
X24	Senior Instructor in Information Technologies Department	10	Head of Information Technologies Department	(blank)	Geopolitical, financial, governance, technology, social, environment
Y25	Professor	10	Head of the Department	Decission regarding the content of the lectures in the subject Computer networks	Financial, geopolitical, social, technology, environmental, governance

Exercise 2

Annex G

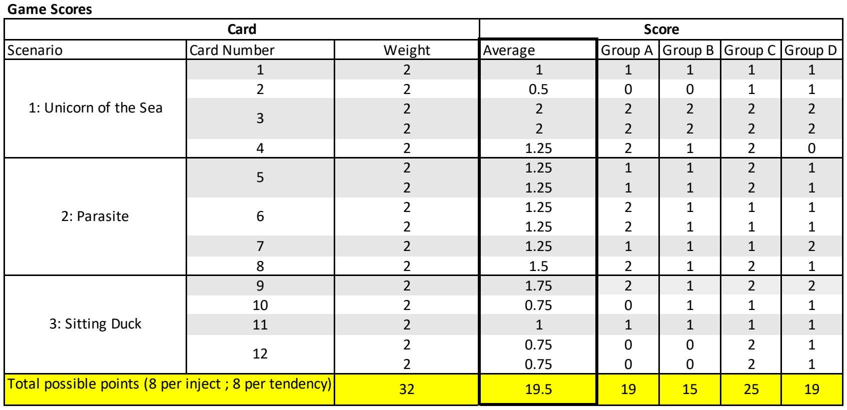
Scenario Questions Results



The Maritime Cybersecurity Game: Methodology

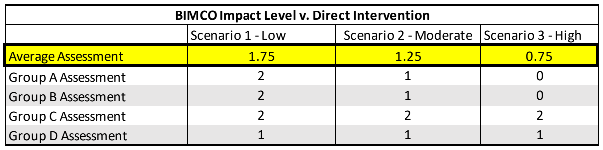
Scenario	Card	Decisionmaking Injects	Response tendencies	Weight	Score	Question	Answer: 0 Point	Answer: 1 Point	Answer: 2 Point
1:Unicorn of the Sea	1	Ecalation	Urgency	2	1	Canadian Authorities arrested five AOS dockworkers in the Port of Iqaluit, in connection with the downed PCT system which delayed AOS Lunchbox. The Dockers Trade Union and the workers' families are requesting a large sum of money from AOS to bail out all five workers from jail and defend them in court. After seeking legal counsel, what do you do?	Delay response as long as possible	Agree to meet with the Trade Union with your decision at the week's end	Immediately agree /decline to pay bail and legal fees for all five workers
	2	Resource Allocation	Private Sector Ownership	2	2	AOS Lunchbox arrives in the Port of Antwerp. Angry customers are waiting for their delayed cargo. Before the cargo can be unloaded, the Port Authority requests a ship inspection be done a cyber expert. You don't have a cyber expert.	You inform the Port Authority they should provide a cyber expert	You ask if the Port Authority knows of a cyber expert AOS can use or hire out	You search for a cyber expert for hire
	3	Reputation Resource Allocation	Direct Intervention	2 2	0 0	AOS donates to a prestigious cybersecurity think-tank. Following the attack at the Port of Iqaluit, AOS's ISO 27001 certification on information security management is revoked. The think-tank has informed you they cannot accept your funding due concerns around best practice and their image, so they terminate your partnership. How are you going to react to this?	Ask ISO 27011 certification body to petition the think-tank on your behalf	Ask think-tank to reconsider due to your history, or find new entity to fund	Use that funding to improve procedures and get certified again, then appeal to think-tank
	4	Time Pressure	Visibility	2	2	70% of cargo being carried by AOS Lunchbox is frozen fish. Halfway to the Port of Antwerp, a container is found leaking water. It seems the delay caused by the cyber-attack upset the cargo refrigeration system, dropping the temperature a few degrees. This means the goods may spoil before they arrive, but they may not spoil.	Don't tell customer of cyber-incident and delay; increase speed and try to pass inspection	Alert customer of cyber-incident and delay, increase speed and try to pass inspection	Alert customer of of cyber-incident and delay, maintain speed and alert them of risk of spoil- confirm all spoiled goods will be reimbursed on inspection.
2: Parasite	5	Escalation	Direct Intervention Private Sector Ownership	2 2	1 1	OSS Dina just arrived to the Port of Algeciras and was arrested under the jurisdiction of Spain. Crew and goods are not allowed to enter or leave the ship, and the ship is not allowed to dock in port. You thought the Peruvian police had connected with Spanish authorities beforehand to avoid such actions, but apparently not.	Ask the Peruvian police to intervene on behalf of OSS to Spanish authorities	Try to arrange three way call between Peruvian police, Spanish police, and OSS	Go to directly to Spanish police with legal aid to demand release of OSS Dina.
	6	Resource Allocation Reputation	Visibility	2 2	2 0	Upon stakeholder request, you agree to significantly increase OSS funding to the charity Cocaine Anonymous and to also increase budget for legal council. These funds will be taken from the annual CEO and executive board bonuses and from a pool reserved for cybersecurity training of staff this year. How will you share this decision?	Omit this from stakeholder report.	Publish complete stakeholder report on OSS website, as is custom	Send the stakeholder report to press and seek wider distribution than normal
	7	Reputation	Urgency	2	1	AOS Stock is plummeting. A press advisor suggests making an international press statement before the close of the day to portray brand stability. The CEO always approves such statements first, but she is unreachable and will remain so until tomorrow due to a time difference. Are you going to go ahead with the statement today or risk losing more points on a stock market?	Delay the press statement a day	Prepare statement but wait for CEO approval (maybe she gets back to you)	Agree to the press statement today
	8	Time Pressure	Private Sector Ownership	2	2	AOS had no choice but to quickly upgrade all legacy ballast systems in their ships. It's an expensive and unplanned investment and needs to be your competitive advantage.	Lobby governments to make this upgrade mandatory across the industry	Strongly advertise you new systems as state-of-the-art for customers	Work with company who did upgrade to patent their technology, on the condition only AOS ships can use it.
3: Sitting Duck	9	Escalation	Visibility	2	1	The Iranian military informed AOS that after inspecting the vicinity, they have found a jamming device on a nearby boat, and linked the entire attack to a regional group known for arms smuggling. Does AOS want to make this information public?	No, do not share this development	Mentioned the involvement of an unnamed group was identified	Yes, share this development
	10	Resource Allocation	Urgency	2	1	It's been a two days and the stranded AOS Jasmine is costing a fortune: High fuel and labor costs, not to mention the late cargo to be reimbursed. On top top of that, AOS has been fined as the seafarers on AOS Jasmine are working too much overtime, in violation of a workers agreement. This has already cost AOS close to the cost of the ransom requested.	Wait as long as it takes, don't pay the ransom.	Give it 24 hours. If it's not resolved, pay the ransom.	Pay the ransomware and move on.
	11	Reputation	Private Sector Ownership	2	1	In the wake of this attack, there is hype around the communication system on AOS Jasmine, which was designed and purchased from Zephyr, an engineering company for autonomous ships. In a radio interview, you state AOS was a victim in part due to new technology. The reporter asks: "Who is responsible to respond to the larger technology issue?"	The government needs to regulate this new technology across the market	It's a combination	Companies like Zephyr that sell such sophisticated technology to companies like AOS need to make sure it is secure
	12	Time Pressure	Direct Intervention Urgency	2 2	1 2	Not all AOS staff, including the CEO, have received cybersecurity training. It your job to ensure that they have, as pointed out by the stakeholders after this attack. They insist a faster response for training be undertaken. How will you address this?	Hire external consultants to host a cybersecurity training program	Pay consultants to design an internal cybersecurity training program	Task existing IT staff with cybersecurity training to design a company-wide internal training program.
Total possible points (8 per inject ; 8 per tendency):				32	18				

Exercise 1



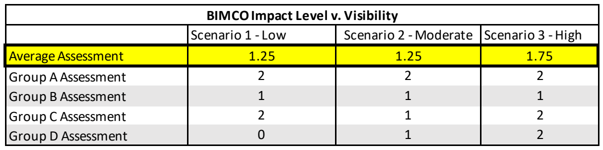
Game Scores

Card			Score				
Scenario	Card Number	Weight	Average	Group A	Group B	Group C	Group D
1: Unicorn of the Sea	1	2	1	1	1	1	1
	2	2	0.5	0	0	1	1
	3	2	2	2	2	2	2
		2	2	2	2	2	2
	4	2	1.25	2	1	2	0
2: Parasite	5	2	1.25	1	1	2	1
		2	1.25	1	1	2	1
	6	2	1.25	2	1	1	1
		2	1.25	2	1	1	1
	7	2	1.25	1	1	1	2
	8	2	1.5	2	1	2	1
3: Sitting Duck	9	2	1.75	2	1	2	2
	10	2	0.75	0	1	1	1
	11	2	1	1	1	1	1
	12	2	0.75	0	0	2	1
		2	0.75	0	0	2	1
Total possible points (8 per inject ; 8 per tendency)		32	19.5	19	15	25	19



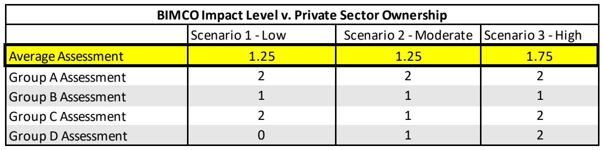
BIMCO Impact Level v. Direct Intervention

	Scenario 1 - Low	Scenario 2 - Moderate	Scenario 3 - High
Average Assessment	1.75	1.25	0.75
Group A Assessment	2	1	0
Group B Assessment	2	1	0
Group C Assessment	2	2	2
Group D Assessment	1	1	1



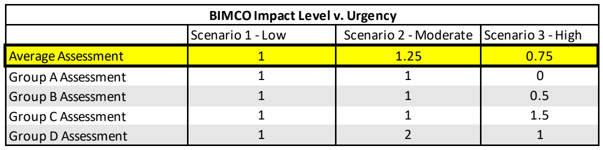
BIMCO Impact Level v. Visibility

	Scenario 1 - Low	Scenario 2 - Moderate	Scenario 3 - High
Average Assessment	1.25	1.25	1.75
Group A Assessment	2	2	2
Group B Assessment	1	1	1
Group C Assessment	2	1	2
Group D Assessment	0	1	2



BIMCO Impact Level v. Private Sector Ownership

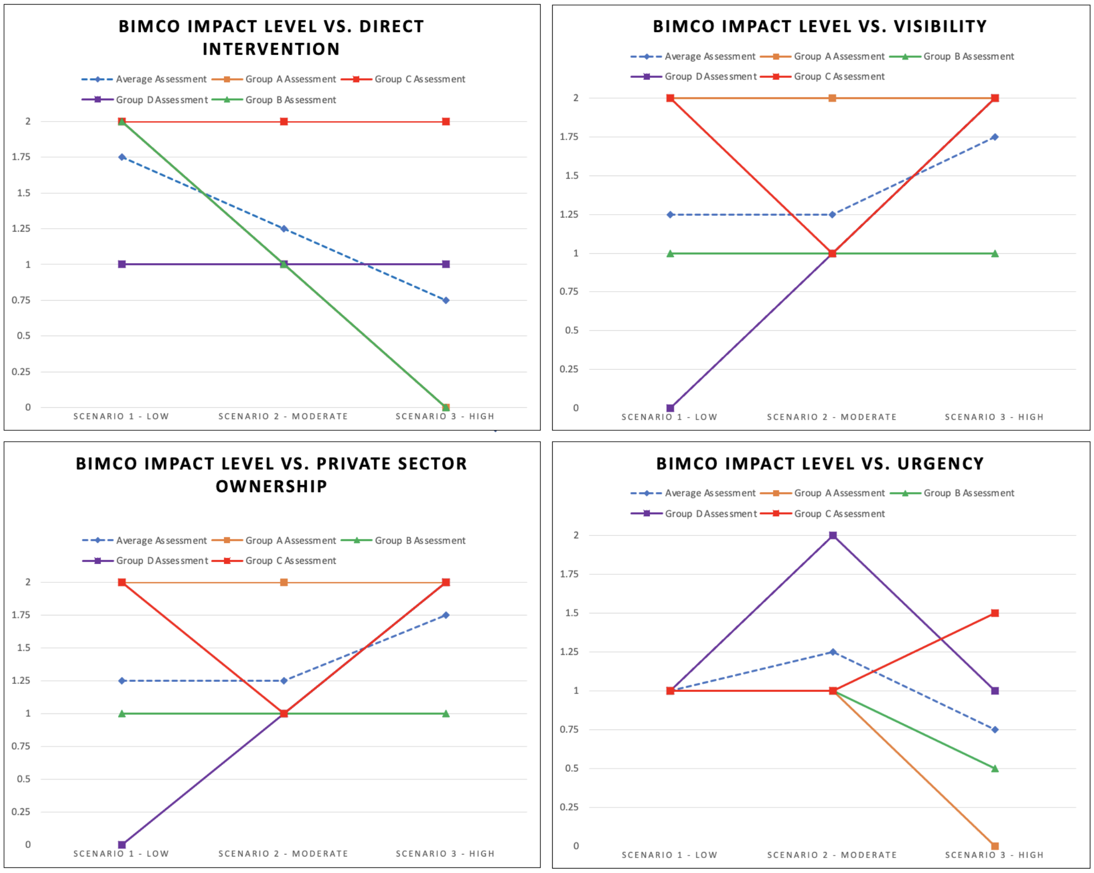
	Scenario 1 - Low	Scenario 2 - Moderate	Scenario 3 - High
Average Assessment	1.25	1.25	1.75
Group A Assessment	2	2	2
Group B Assessment	1	1	1
Group C Assessment	2	1	2
Group D Assessment	0	1	2



BIMCO Impact Level v. Urgency

	Scenario 1 - Low	Scenario 2 - Moderate	Scenario 3 - High
Average Assessment	1	1.25	0.75
Group A Assessment	1	1	0
Group B Assessment	1	1	0.5
Group C Assessment	1	1	1.5
Group D Assessment	1	2	1

Exercise 1

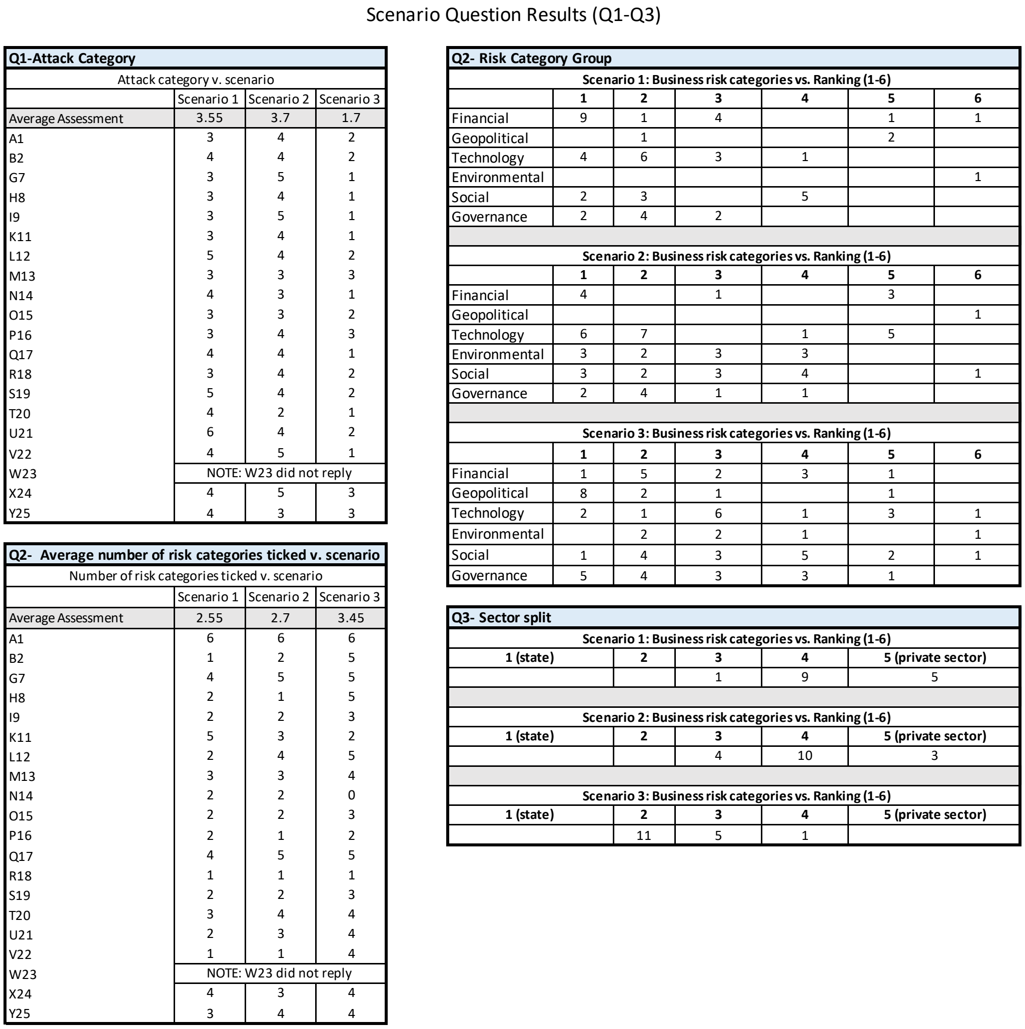

BIMCO IMPACT LEVEL VS. DIRECT INTERVENTION

BIMCO IMPACT LEVEL VS. VISIBILITY

BIMCO IMPACT LEVEL VS. PRIVATE SECTOR OWNERSHIP

BIMCO IMPACT LEVEL VS. URGENCY

Exercise 1



Scenario Question Results (Q1-Q3)

Q1-Attack Category

Attack category v. scenario

	Scenario 1	Scenario 2	Scenario 3
Average Assessment	3.55	3.7	1.7
A1	3	4	2
B2	4	4	2
G7	3	5	1
H8	3	4	1
I9	3	5	1
K11	3	4	1
L12	5	4	2
M13	3	3	3
N14	4	3	1
O15	3	3	2
P16	3	4	3
Q17	4	4	1
R18	3	4	2
S19	5	4	2
T20	4	2	1
U21	6	4	2
V22	4	5	1
W23	NOTE: W23 did not reply		
X24	4	5	3
Y25	4	3	3

Q2- Average number of risk categories ticked v. scenario

Number of risk categories ticked v. scenario

	Scenario 1	Scenario 2	Scenario 3
Average Assessment	2.55	2.7	3.45
A1	6	6	6
B2	1	2	5
G7	4	5	5
H8	2	1	5
I9	2	2	3
K11	5	3	2
L12	2	4	5
M13	3	3	4
N14	2	2	0
O15	2	2	3
P16	2	1	2
Q17	4	5	5
R18	1	1	1
S19	2	2	3
T20	3	4	4
U21	2	3	4
V22	1	1	4
W23	NOTE: W23 did not reply		
X24	4	3	4
Y25	3	4	4

Q2- Risk Category Group

Scenario 1: Business risk categories vs. Ranking (1-6)

	1	**2**	**3**	**4**	**5**	**6**
Financial	9	1	4		1	1
Geopolitical		1			2	
Technology	4	6	3	1		
Environmental						1
Social	2	3		5		
Governance	2	4	2			

Scenario 2: Business risk categories vs. Ranking (1-6)

	1	**2**	**3**	**4**	**5**	**6**
Financial	4		1		3	
Geopolitical						1
Technology	6	7		1	5	
Environmental	3	2	3	3		
Social	3	2	3	4		1
Governance	2	4	1	1		

Scenario 3: Business risk categories vs. Ranking (1-6)

	1	**2**	**3**	**4**	**5**	**6**
Financial	1	5	2	3	1	
Geopolitical	8	2	1		1	
Technology	2	1	6	1	3	1
Environmental		2	2	1		1
Social	1	4	3	5	2	1
Governance	5	4	3	3	1	

Q3- Sector split

Scenario 1: Business risk categories vs. Ranking (1-6)

1 (state)	**2**	**3**	**4**	**5 (private sector)**
		1	9	5

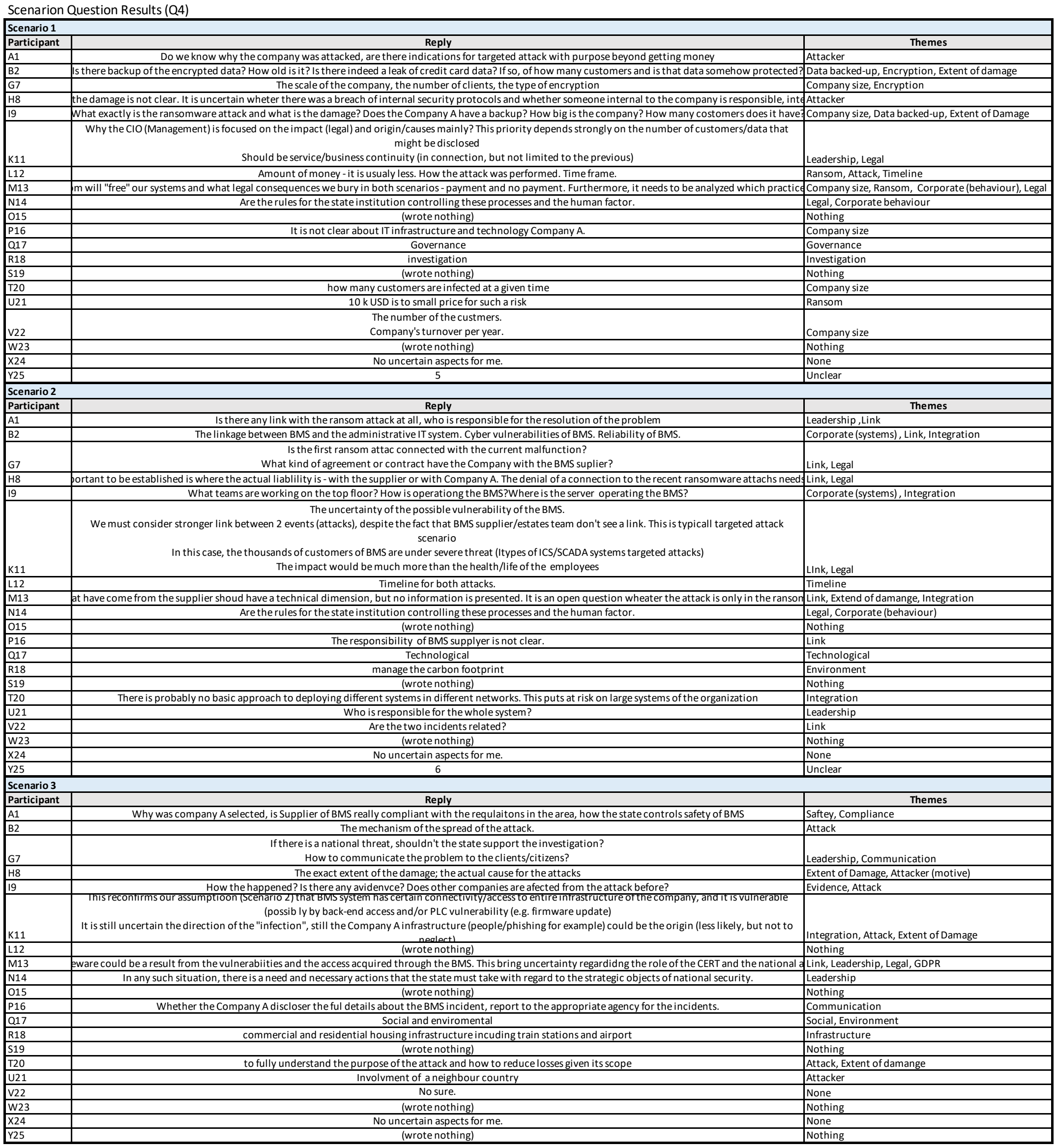
Scenario 2: Business risk categories vs. Ranking (1-6)

1 (state)	**2**	**3**	**4**	**5 (private sector)**
		4	10	3

Scenario 3: Business risk categories vs. Ranking (1-6)

1 (state)	**2**	**3**	**4**	**5 (private sector)**
	11	5	1	

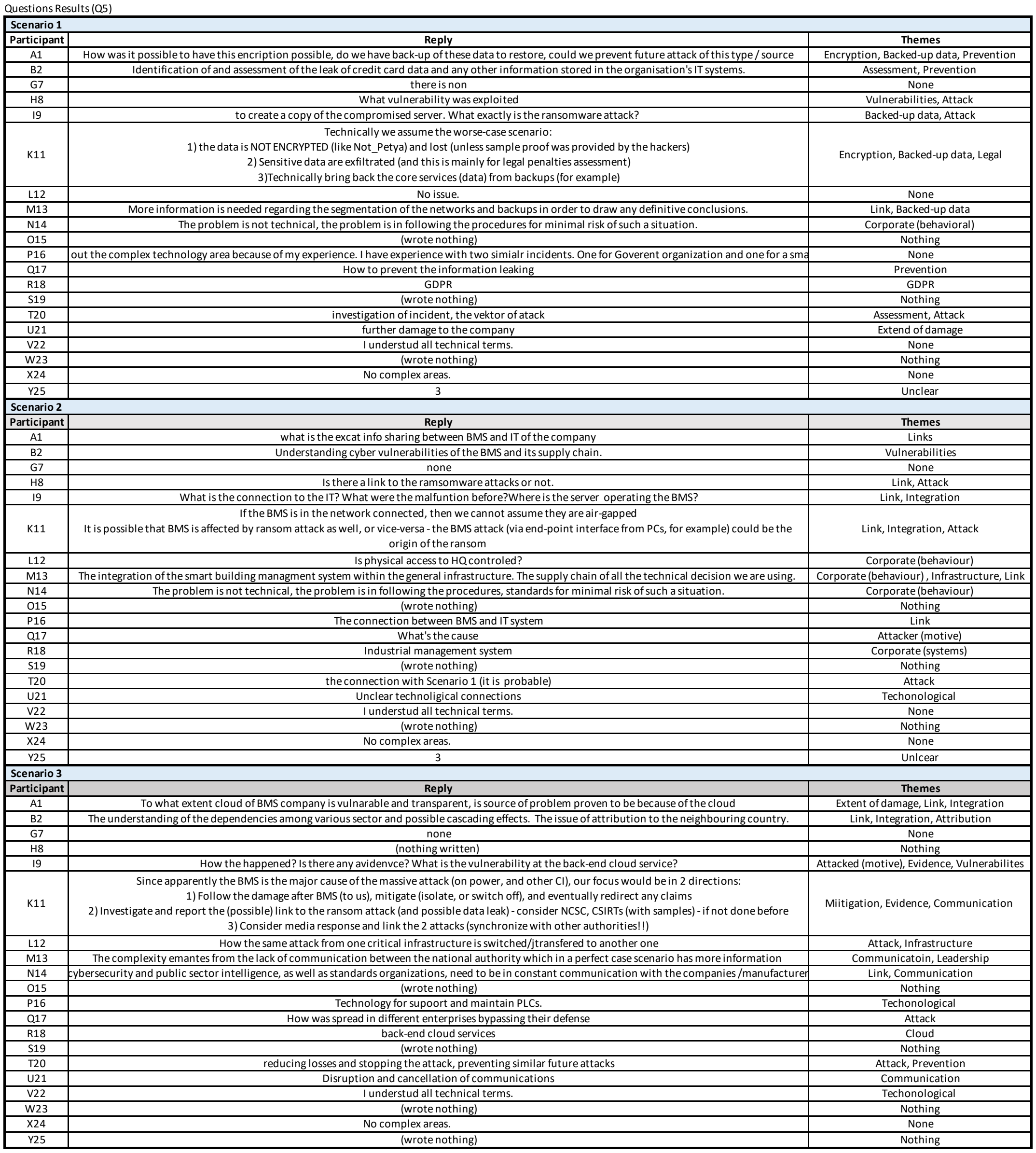
Exercise 2



Scenarion Question Results (Q4)

Scenario 1		
Participant	**Reply**	**Themes**
A1	Do we know why the company was attacked, are there indications for targeted attack with purpose beyond getting money	Attacker
B2	Is there backup of the encrypted data? How old is it? Is there indeed a leak of credit card data? If so, of how many customers and is that data somehow protected?	Data backed-up, Encryption, Extent of damage
G7	The scale of the company, the number of clients, the type of encryption	Company size, Encryption
H8	the damage is not clear. It is uncertain wheter there was a breach of internal security protocols and whether someone internal to the company is responsible, inte	Attacker
I9	What exactly is the ransomware attack and what is the damage? Does the Company A have a backup? How big is the company? How many costomers does it have?	Company size, Data backed-up, Extent of Damage
K11	Why the CIO (Management) is focused on the impact (legal) and origin/causes mainly? This priority depends strongly on the number of customers/data that might be disclosed Should be service/business continuity (in connection, but not limited to the previous)	Leadership, Legal
L12	Amount of money - it is usualy less. How the attack was performed. Time frame.	Ransom, Attack, Timeline
M13	m will "free" our systems and what legal consequences we bury in both scenarios - payment and no payment. Furthermore, it needs to be analyzed which practice	Company size, Ransom, Corporate (behaviour), Legal
N14	Are the rules for the state institution controlling these processes and the human factor.	Legal, Corporate behaviour
O15	(wrote nothing)	Nothing
P16	It is not clear about IT infrastructure and technology Company A.	Company size
Q17	Governance	Governance
R18	investigation	Investigation
S19	(wrote nothing)	Nothing
T20	how many customers are infected at a given time	Company size
U21	10 k USD is to small price for such a risk	Ransom
V22	The number of the custmers. Company's turnover per year.	Company size
W23	(wrote nothing)	Nothing
X24	No uncertain aspects for me.	None
Y25	5	Unclear
Scenario 2		
Participant	**Reply**	**Themes**
A1	Is there any link with the ransom attack at all, who is responsible for the resolution of the problem	Leadership ,Link
B2	The linkage between BMS and the administrative IT system. Cyber vulnerabilities of BMS. Reliability of BMS.	Corporate (systems) , Link, Integration
G7	Is the first ransom attac connected with the current malfunction? What kind of agreement or contract have the Company with the BMS suplier?	Link, Legal
H8	portant to be established is where the actual liablility is - with the supplier or with Company A. The denial of a connection to the recent ransomware attachs needs	Link, Legal
I9	What teams are working on the top floor? How is operationg the BMS?Where is the server operating the BMS?	Corporate (systems) , Integration
K11	The uncertainty of the possible vulnerability of the BMS. We must consider stronger link between 2 events (attacks), despite the fact that BMS supplier/estates team don't see a link. This is typicall targeted attack scenario In this case, the thousands of customers of BMS are under severe threat (Itypes of ICS/SCADA systems targeted attacks) The impact would be much more than the health/life of the employees	LInk, Legal
L12	Timeline for both attacks.	Timeline
M13	at have come from the supplier shoud have a technical dimension, but no information is presented. It is an open question wheater the attack is only in the ranson	Link, Extend of damange, Integration
N14	Are the rules for the state institution controlling these processes and the human factor.	Legal, Corporate (behaviour)
O15	(wrote nothing)	Nothing
P16	The responsibility of BMS supplyer is not clear.	Link
Q17	Technological	Technological
R18	manage the carbon footprint	Environment
S19	(wrote nothing)	Nothing
T20	There is probably no basic approach to deploying different systems in different networks. This puts at risk on large systems of the organization	Integration
U21	Who is responsible for the whole system?	Leadership
V22	Are the two incidents related?	Link
W23	(wrote nothing)	Nothing
X24	No uncertain aspects for me.	None
Y25	6	Unclear
Scenario 3		
Participant	**Reply**	**Themes**
A1	Why was company A selected, is Supplier of BMS really compliant with the requlaitons in the area, how the state controls safety of BMS	Saftey, Compliance
B2	The mechanism of the spread of the attack.	Attack
G7	If there is a national threat, shouldn't the state support the investigation? How to communicate the problem to the clients/citizens?	Leadership, Communication
H8	The exact extent of the damage; the actual cause for the attacks	Extent of Damage, Attacker (motive)
I9	How the happened? Is there any avidenvce? Does other companies are afected from the attack before?	Evidence, Attack
K11	This reconfirms our assumptioon (Scenario 2) that BMS system has certain connectivity/access to entire infrastructure of the company, and it is vulnerable (possib ly by back-end access and/or PLC vulnerability (e.g. firmware update) It is still uncertain the direction of the "infection", still the Company A infrastructure (people/phishing for example) could be the origin (less likely, but not to neglect)	Integration, Attack, Extent of Damage
L12	(wrote nothing)	Nothing
M13	eware could be a result from the vulnerabiities and the access acquired through the BMS. This bring uncertainty regardidng the role of the CERT and the national a	Link, Leadership, Legal, GDPR
N14	In any such situation, there is a need and necessary actions that the state must take with regard to the strategic objects of national security.	Leadership
O15	(wrote nothing)	Nothing
P16	Whether the Company A discloser the ful details about the BMS incident, report to the appropriate agency for the incidents.	Communication
Q17	Social and enviromental	Social, Environment
R18	commercial and residential housing infrastructure incuding train stations and airport	Infrastructure
S19	(wrote nothing)	Nothing
T20	to fully understand the purpose of the attack and how to reduce losses given its scope	Attack, Extent of damange
U21	Involvment of a neighbour country	Attacker
V22	No sure.	None
W23	(wrote nothing)	Nothing
X24	No uncertain aspects for me.	None
Y25	(wrote nothing)	Nothing

Exercise 2



Questions Results (Q5)

Scenario 1

Participant	Reply	Themes
A1	How was it possible to have this encription possible, do we have back-up of these data to restore, could we prevent future attack of this type / source	Encryption, Backed-up data, Prevention
B2	Identification of and assessment of the leak of credit card data and any other information stored in the organisation's IT systems.	Assessment, Prevention
G7	there is non	None
H8	What vulnerability was exploited	Vulnerabilities, Attack
I9	to create a copy of the compromised server. What exactly is the ransomware attack?	Backed-up data, Attack
K11	Technically we assume the worse-case scenario: 1) the data is NOT ENCRYPTED (like Not_Petya) and lost (unless sample proof was provided by the hackers) 2) Sensitive data are exfiltrated (and this is mainly for legal penalties assessment) 3)Technically bring back the core services (data) from backups (for example)	Encryption, Backed-up data, Legal
L12	No issue.	None
M13	More information is needed regarding the segmentation of the networks and backups in order to draw any definitive conclusions.	Link, Backed-up data
N14	The problem is not technical, the problem is in following the procedures for minimal risk of such a situation.	Corporate (behavioral)
O15	(wrote nothing)	Nothing
P16	out the complex technology area because of my experience. I have experience with two simialr incidents. One for Goverent organization and one for a sma	None
Q17	How to prevent the information leaking	Prevention
R18	GDPR	GDPR
S19	(wrote nothing)	Nothing
T20	investigation of incident, the vektor of atack	Assessment, Attack
U21	further damage to the company	Extend of damage
V22	I understud all technical terms.	None
W23	(wrote nothing)	Nothing
X24	No complex areas.	None
Y25	3	Unclear

Scenario 2

Participant	Reply	Themes
A1	what is the excat info sharing between BMS and IT of the company	Links
B2	Understanding cyber vulnerabilities of the BMS and its supply chain.	Vulnerabilities
G7	none	None
H8	Is there a link to the ramsomware attacks or not.	Link, Attack
I9	What is the connection to the IT? What were the malfuntion before?Where is the server operating the BMS?	Link, Integration
K11	If the BMS is in the network connected, then we cannot assume they are air-gapped It is possible that BMS is affected by ransom attack as well, or vice-versa - the BMS attack (via end-point interface from PCs, for example) could be the origin of the ransom	Link, Integration, Attack
L12	Is physical access to HQ controled?	Corporate (behaviour)
M13	The integration of the smart building managment system within the general infrastructure. The supply chain of all the technical decision we are using.	Corporate (behaviour) , Infrastructure, Link
N14	The problem is not technical, the problem is in following the procedures, standards for minimal risk of such a situation.	Corporate (behaviour)
O15	(wrote nothing)	Nothing
P16	The connection between BMS and IT system	Link
Q17	What's the cause	Attacker (motive)
R18	Industrial management system	Corporate (systems)
S19	(wrote nothing)	Nothing
T20	the connection with Scenario 1 (it is probable)	Attack
U21	Unclear technoligical connections	Techonological
V22	I understud all technical terms.	None
W23	(wrote nothing)	Nothing
X24	No complex areas.	None
Y25	3	Unlcear

Scenario 3

Participant	Reply	Themes
A1	To what extent cloud of BMS company is vulnarable and transparent, is source of problem proven to be because of the cloud	Extent of damage, Link, Integration
B2	The understanding of the dependencies among various sector and possible cascading effects. The issue of attribution to the neighbouring country.	Link, Integration, Attribution
G7	none	None
H8	(nothing written)	Nothing
I9	How the happened? Is there any avidenvce? What is the vulnerability at the back-end cloud service?	Attacked (motive), Evidence, Vulnerabilites
K11	Since apparently the BMS is the major cause of the massive attack (on power, and other CI), our focus would be in 2 directions: 1) Follow the damage after BMS (to us), mitigate (isolate, or switch off), and eventually redirect any claims 2) Investigate and report the (possible) link to the ransom attack (and possible data leak) - consider NCSC, CSIRTs (with samples) - if not done before 3) Consider media response and link the 2 attacks (synchronize with other authorities!!)	Miitigation, Evidence, Communication
L12	How the same attack from one critical infrastructure is switched/jtransfered to another one	Attack, Infrastructure
M13	The complexity emantes from the lack of communication between the national authority which in a perfect case scenario has more information	Communicatoin, Leadership
N14	cybersecurity and public sector intelligence, as well as standards organizations, need to be in constant communication with the companies /manufacturer	Link, Communication
O15	(wrote nothing)	Nothing
P16	Technology for supoort and maintain PLCs.	Techonological
Q17	How was spread in different enterprises bypassing their defense	Attack
R18	back-end cloud services	Cloud
S19	(wrote nothing)	Nothing
T20	reducing losses and stopping the attack, preventing similar future attacks	Attack, Prevention
U21	Disruption and cancellation of communications	Communication
V22	I understud all technical terms.	Techonological
W23	(wrote nothing)	Nothing
X24	No complex areas.	None
Y25	(wrote nothing)	Nothing

Exercise 2