TU Delft

Delft University of Technology

Executive decision-makers

a scenario-based approach to assessing organizational cyber-risk perception

Parkin, Simon; Kuhn, Kristen; Shaikh, Siraj A.

DOI
10.1093/cybsec/tyad018

Publication date
2023

Document Version
Final published version

Published in
Journal of Cybersecurity

Citation (APA)
Parkin, S., Kuhn, K., & Shaikh, S. A. (2023). Executive decision-makers: a scenario-based approach to assessing organizational cyber-risk perception. *Journal of Cybersecurity*, *9*(1), Article tyad018. https://doi.org/10.1093/cybsec/tyad018

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.
For technical reasons the number of authors shown on this cover page is limited to a maximum of 10.

JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2023, 1–13
https://doi.org/10.1093/cybsec/tyad018
Research paper

Research paper

Executive decision-makers: a scenario-based approach to assessing organizational cyber-risk perception

Simon Parkin [1], Kristen Kuhn[2] and Siraj A. Shaikh [3,4,*]

[1]Faculty of Technology, Policy and Management, TU Delft, Jaffalaan 5, 2628 BX, Delft, the Netherlands, [2]Centre for Trust, Peace and Social Relations (CTPSR), Coventry University, Coventry, CV1 5FB, United Kingdom, [3]Systems Security Group (SSG), Department of Computer Science, Swansea University, Bay Campus, Fabian Way, Swansea, SA1 8EN, United Kingdom and [4]Research Centre on Security, Rule of Law and High TechnologiesResearch Centre on Security, Rule of Law and High Technologiesniversidad Nebrija, Madrid 28015, Spain

*Correspondence address. Systems Security Group (SSG), Department of Computer Science, Swansea University, Bay Campus, Fabian Way, Swansea, SA1 8EN, United Kingdom. Tel: +44 7939 233 995; E-mail: s.a.shaikh@swansea.ac.uk

Received 28 December 2022; revised 1 June 2023; accepted 24 July 2023

Abstract

The executive leadership in corporate organizations is increasingly challenged with managing cyber-risks, as an important part of wider business risk management. Cyber-risks are complex, with the threat landscape evolving, including digital infrastructure issues such as trust in networked supply chains, and emerging technologies. Moreover, engaging organizational leadership to assess for risk management is also difficult. This paper reports on a scenario-driven, workshop-based study undertaken with executive leadership to assess for cybersecurity and cyber-risk perception related to preparation for, and response to, potential incidents. The study involves leadership members at a large public–private organization. Our approach utilizes scenarios, which are structured in their design to explore and analyse aspects of business risk, risk ownership, technological complexity, and uncertainty faced by an organizational leadership. The method offers a means to engage with leadership at real-world organizations, capturing capacity and insights to manage business risks due to cyberattacks.

Key words: security management, decision making, business continuity, risk analysis

Introduction

As enterprise digitization and automation play an increasingly central role in how organizations are operated, the security of networked systems, services, and corporate IT is becoming increasingly critical to business continuity. Cybersecurity is then increasingly relevant as a responsibility of decision-making stakeholders in organizations [1], including senior organizational leadership [2].

Notable forms of cyber-related attacks include destructive malware (as with Maersk [3]) and ransomware attacks (as with Norsk Hydro [4]). In early 2021, Colonial Pipeline was impacted by ransomware, with the US government then acting to retrieve some of the ransom [5], highlighting the complex, multistakeholder nature of cybersecurity decisions. Cybersecurity incidents can last for some time, incurring increased costs and disruption to both the business and customers. The understanding of incidents also evolves rapidly under conditions of uncertainty as details emerge. It is then key that executive leadership are prepared for managing incidents where there is an evolving cybersecurity element.

The understanding of risk arising out of such incidents is therefore important, and is the core of the focus of this paper. Such an understanding would involve at least three aspects of risk in businesses to be assessed including: risk ownership (who is best placed to take action); type of risk (how is the risk recognized in a way that it can be responded to, for instance, by following regulated procedures or adapting to novel crises); the level of risk (with it being security, the severity and urgency, which determines the planning). If such *resilience* is planned into business procedures, this boosts ability to weather future emergencies [6].

© The Author(s) 2023. Published by Oxford University Press. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted reuse, distribution, and reproduction in any medium, provided the original work is properly cited.

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad018/7246580 by Delft University of Technology user on 15 September 2023

Our approach lays down the foundations for a systematic scenario-based risk exploration amongst senior decision-makers in organizations. The use of scenarios have the advantage that cybersecurity risks new to the organization could be considered in terms of perceived relevance, responsibilities, and necessary responses (rather than leaving it to responding to such novel risks in a more *ad-hoc* fashion when they happen). Participants may already have what they believe to be an appropriate response, where our approach is also an opportunity to assure themselves that they are prepared.

Our approach is also tailored to our target audience, to ensure that the format for engagement is suited to them in terms of time constraints, level of technical knowledge, and weaving emerging cybersecurity risks with the business risk landscape that they would be familiar with.

Here, we explore perceptions of cybersecurity-related risks at the highest levels of an organization relative to other business concerns. Within this, we also investigate how cybersecurity is perceived within new or existing business continuity and incident response processes, with a view to informing business preparedness [1,7]. Informed by existing research [7], we engaged with senior governance and business continuity decision-makers through a structured, scenario-driven and repeatable exercise intended for executive decision-makers. These planning activities aim to inform 'practices for preparedness' [6], specifically in the cybersecurity domain.

This paper makes a contribution towards capacity to practise such preparedness, and sets out to address the following research questions:

- **RQ1:** Does a scenario-based approach to articulation of business risks (arising out of cyber-risks) effectively capture insights from business decision-makers?
  This is founded on a systematic approach to the construction of scenarios.
- **RQ2:** Do decision-makers across the wider business perceive whether cyber-risk relates to their domain of decisions?
  This would include assessing the perceived nature of risks and attribution of risk ownership.

We conducted a half-day online workshop, with nine members of executive leadership of a large public–private sector organization in a developed economy, which provides a range of services including postal and financial services. The organization has dedicated responsibilities for the General Data Protection Regulation (GDPR) compliance, incident reporting, and business continuity preparedness. During the workshop, participants were presented with progressions of a cybersecurity incident as a sequence of four scenarios (ransomware, control system malfunction, power and connectivity outage, nation–state disruption). For scenarios to appear realistic and at the same time novel and engaging to participants, the scenario design leverages the notion of 'near future' [8] scenarios. Such an approach has been used in war games and strategy exercises, to draw on existing experiences.

We found that our scenario design resonated with participants, prompting consideration of the role of cyber-risks relevant to other kinds of risks, such as critical services and the potential of physical harm. The role of crisis management processes and task forces was highlighted by participants, as a means to coordinate the complexity of managing cyber-related incidents and to align the perspectives of different organization-internal stakeholders.

The rest of this paper is organized as follows: background and related work are discussed in the 'Background and related work' section; our survey and workshop methodology are detailed in the 'Methodology' section, with the results of the workshop presented in the 'Results' section. Discussion, including consideration of limitations, appears in the 'Discussion' section, with closing remarks and future work detailed in the 'Conclusion and future work' section.

Background and related work

Where cybersecurity research has investigated high-level decisions about how the security of organizations and systems are managed, it has mainly focused at the level of strategic management of security and the experiences of senior security managers [9–11]. Research has seldom reached the level of executive decision-makers interacting with other functions *including* cybersecurity, at the highest level of an organization.

We frame 'executive' decision-makers to be individuals who make decisions, which drive the direction and strategy of an organization. Where *'each board needs to set its own direction and tone for cyber security'* [12], we regard this as being embodied by the ways in which top-level strategic decision-making includes cybersecurity. While executive boards take many forms and may operate varying reporting structures [9], here, we focuse on governance-related decisions, which involve multiple executive decision-makers of an organization, where cybersecurity events may enter that purview (as with e.g. ransomware or malware attacks targeting individual organizations). Executive decision-makers have a need to address multiple directives at once, foremost that the organization is secure while also being able to operate in its primary capacity (as may be determined by the sector and supply chains it operates within).

Top-level decision-making involves complex interactions between leadership teams [13], around 'episodic' decisions and strategic issues. Risk perception is relevant for organizational leadership because it influences their decision-making [14]. An understanding of the perception of cyber-related risks at senior decision-making levels—including its perceived place relative to other risk management apparatus—can inform cybersecurity incident response. Simulations are a means to test preparedness for crises, but also for decision-makers to develop *experiential learning* [15]. Within cybersecurity, this preparation can include scenario-based methods, which bring together objectives, scenario injects, observation methods, and evaluation methods [16].

Related work

Hussain et al. [16] critically review an extensive set of scenario-based games and exercises for cybersecurity. Using a strict criteria where the target participants are engaged in decision-making, they shortlist to under four dozen exercises. Most of these exercises focus on highly technical scenarios, where the risks are described in terms of digital assets and the decision space ranges over technical countermeasures. Notably, our intention to focus on business risks with senior executive participation from the same organization remains unmatched across the reviewed approaches.

In terms of assessment of risk perception, the majority of such exercises are aimed at a policy audience where an assessment of risk perception is within a political or official governance framework. The most well known of these is the Cyber 9/12 Strategy Challenge [17] where large-scale cyberattacks are stipulated as highly detailed scenarios (*albeit* tabletop), and participants—drawn from public policy training schools—are challenged to identify responses within the NATO and EU governance structures. Corporate organizations are not the target audience, even though the participants are challenged with coordinating across public and private sectors as part of the response to scenarios. The exercise runs over multiple days organized

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad018/7246580 by Delft University of Technology user on 15 September 2023

by the Atlantic Council [18] and Geneva Centre for Security Policy [19].

Approaches studying relevant decision-making within corporate organizations amount to very few. One includes a simulation approach by Jalali et al. [20] where a fictional company is used as a scenario for group of experienced and inexperience cybersecurity managers to plan for proactive return on investment. A simulation framework is used to assess investment decisions towards maximizing cybersecurity-related capacity development and risk mitigation. The participants come from different organizations and also include graduate students.

Shreeve et al. [1] leveraged a tabletop role-playing game themed around cyber-physical systems, to study the decision-making processes of participants from a wide range of backgrounds within organizations (including board members, finance, and legal). The authors identified that team diversity did not necessarily influence how cybersecurity problems were faced, and that cybersecurity specialists would tend to favour new technologies in search of a solution. In similar work, Shreeve et al. [21] conducted another examination of table-top role-playing dynamics, focusing on the role of intuition and experience in decision-making, and finding that approaches resembling the logic of espoused cyber-risk management emerge in those players who lack expertise. Here, we explore the perceived role of different stakeholders with a view to incident management and business continuity, which includes a cybersecurity element, finding that participants contrast unfolding cyber-risk situations with how they would manage other forms of incidents.

Through a survey, Rhee et al. [22] explore whether top-level managers exhibit an optimistic bias towards their perception of security risks related to their organization. The authors found an appreciation for the interdependence between organizations and control of risks relative to business partners and comparable companies. Here, we explore how management processes for incidents with a cybersecurity element may act to control and coordinate response to emerging risks.

Merrill [23] proposes 'security fictions' as a vehicle for using speculative design to explore the identification of security threats, specifically with software developers. Although a different participant community, there are parallels with the design of fictional events around specific cybersecurity threats. Merrill comments that 'threat identification is a socially situated practice', where here we relate cybersecurity as one of many concerns in managing an organisation and its role in society.

Methodology

In this section, we describe the design of our scenario exercise, the distinct dimensions within the scenario designs, study protocol, and a summary description of the study participants. We adapt an existing methodology for scenario design [7], focusing here on a broad group of executive decision-makers with a variety of roles in one large organization, as opposed to a community of executive cybersecurity decision-makers based across multiple organizations.

Executive decision-makers respond more naturally to a *descriptive* perspective on risk [24], rather than a normative description of costs and probabilities. This has been seen elsewhere within the security domain [25]. To explore risk *judgements* at this level of decision-making, we expose participants to *systematically constructed scenarios*, which describe 'near future' events (see the 'Scenario design for executive cyber-risks' section). Risk decisions at this level involve dimensions such as *'uncertainty, ignorance, incomplete knowledge, and ambiguity'* [24], where these aspects inform parameters in scenario design (see the 'Scenario dimensions' section). The scenarios are designed to encapsulate a complete description of the process of risk taking [24], combining the Definition, Attitudes, and Evaluation around pertinent risks.

Scenario design for executive cyber-risks

In designing the scenarios, we were mindful of the need to maintain ecological validity [26]. Participants will understand that the scenario is not real, but to explore RQ1, efforts were made to develop scenarios, which would resonate with the sector the participating organization operates in (in this case, centred around postal services). As such, the participants can consider the scenario as if it were a real-life brief of an emerging situation.

A set of four scenarios was developed to act as discrete progressions of a potential incident involving a hypothetical 'Company A', as in Tables 1 and 2. In sequence, the scenarios explore escalation of complexity and ambiguity, building on preceding scenarios.

The design of the scenarios was informed by the authors' knowledge of IT systems and relevant cybersecurity issues for organizations, relative to the sector that the organization operates in. A knowledgeable practitioner with a wealth of experience at the executive level also provided feedback on the design of the scenarios (see the 'Study protocol' section); given the challenges in finding participants at this level and optimizing use of their time, this approach was taken instead of a pilot session (as would normally occur for a study involving human participants).

The sequence of scenarios embody varying degrees of impact. In terms of impact from cyber-risk, this represents a general escalation from low (S1) to medium (S2 and S3) to high (S4), as shown in Tables 1 and 2. Scenarios S2 and S3 are designed to explore the space between 'extremes' of low and high, as variations on 'medium' severity. The escalation of impacts and risk, as in Table 3, is exemplified as a complex mix of people and systems, which may be affected by the events possible within and around each scenario (given the interacting elements of technical complexity and uncertainty within them).

Scenario dimensions

The scenario dimensions are adapted from the work described in ref. [7], in which the dimensions were used to elicit views about business risks related to cybersecurity. We posit that this capability is applicable also to discussions with businesses risk owners who may be impacted by cybersecurity incidents, to answer our second research question (RQ2). The columns in Table 3 describe the dimensions along which scenarios are designed, and the rows show the range of elements which each scenario is expected to evoke. Scenario dimensions include: risk externalities (including other stakeholders affected) [27]; stakeholder management; anticipated risks; areas of uncertainty; technical areas of complexity, and; attack classification. For each scenario, Table 3 illustrates responses that the authors anticipate for each scenario. Questions to participants prompt them to classify and describe each scenario along these dimensions (as in the Appendix).

Anticipated risks

We assess the scenarios for particular categories of business risk, as per the *Cambridge Taxonomy of Business Risks* [28]. These risk categories embody a complete range of risks relevant to businesses, as follows:

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad018/7246580 by Delft University of Technology user on 15 September 2023

Table 1: Scenarios 1 and 2, written as a continuous narrative around an organization referred to as 'Company A'.

Scenario 1—'ransomware' (Sc-Ransom)
• 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$500,000 within 3 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—'control system malfunction' (Sc-Pods)
• Company A operates a fleet of autonomous delivery pods, supporting one of the main functions, it provides of delivering post, in a number of cities across the country. This is a relatively new service that has been operational only for the past year, and Company A has rolled out deployment of the technology across major cities (with well over half of the deliveries being serviced using these pods across the four biggest cities). • Three days after the incident (in Scenario 1), the Fleet Operations at Company A has reported a malfunction with the Central Control System (CCS) that remotely manages the autonomous delivery pods in the country's capital. The malfunction has caused much of the pods delivery network to cease operation, with a few reports of the pods showing loss of control and crashing into other pods, delivery operators, and the pod parking bays. As a result, three pods have reported to have been damaged, and two operators have been slightly injured. Also, this has led to manual switchover of deliveries in the city, causing severe delays to postal operations. The manual switchover has meant relying on delivery drivers (with shortage of vehicles and drivers to manage) and delivery on foot. • The IT Team has confirmed that the CCS 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 (in Scenario 1), has no link to the CCS even if both are connected to the corporate IT network. • The Fleet Operations have had the suppliers of the delivery pods investigate the malfunction. The pod 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 participants start with Scenario 1, which then escalates in three subsequent rounds through Scenarios 2–4 as a series of developments. We have given the scenarios short-hand names for reference, though we did not explicitly refer to them with these names during the workshop so as not to influence interpretation.

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

Attack classification

An 'attack classification' scale was included, to capture how participants regard the severity of the scenario. For this measure, we adopted the scale for cyberattack incident categorization proposed by the UK's National Cyber Security Centre (NCSC) [29]. By designing—and in turn, discussing—scenarios according to this scale, we are able to arrange scenarios and structure engagement along a journey of increasing incident severity (from S1 through to S4). The scale was shared with participants before they were presented with the scenarios, as follows:

– *Category 1 (National cyber emergency)*. Causes sustained disruption of essential services or affects national security, leading to severe economic or social consequences or to 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 organization or on wider / local government, or which poses a considerable risk to central government or essential services;
– *Category 4 (Substantial incident)*. Has a serious impact on a medium-sized organization, or which poses a considerable risk to a large organization or wider / local government;
– *Category 5 (Moderate incident)*. Poses considerable risk to a small or medium-sized organization, or preliminary indications of cyber activity against a large organization or the government;
– *Category 6 (Localized incident)*. Poses considerable risk to an individual, or preliminary indications of cyber activity against a small or medium-sized organization.

Complexity, uncertainty, and responsibility

We include open questions for each scenario, which prompt participants to identify where they see notable areas of complexity and uncertainty. These elements of decision-making have been highlighted as being critical at the executive level [24]. We also ask participants to indicate the perceived scope of responsibility for the incident on a scale that shifts from wholly private sector to state-owned, with a mix at the centre (where this is distinct from the classification of cybersecurity incident as above).

Study protocol

An online workshop was conducted in May 2021. The entire author team, participants, and the aforementioned knowledgeable practitioner (acting for the most part as an observer) joined an online video conferencing session. The time for the entire study was preagreed to a defined slot with the participants. This was a rare opportunity where we secured all the relevant stakeholders from the organization to come together and engage in the study in full.

Before the workshop event, the authors confirmed that consent forms had been provided and returned. Participants were also asked

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad018/7246580 by Delft University of Technology user on 15 September 2023

Table 2: Scenarios 3 and 4, following on from Scenarios 1 and 2.

Scenario 3—'power and connectivity outage' (Sc-Power)
• Four days after the incident (in Scenario 2), Fleet Operations at Company A have now advised the CEO that limited operations of the delivery pods are ready to commence. An early joint investigation with the pods supplier has led them to assess the system to be safe and ready for operations; the entire system has been bootstrapped and cleared of any potentially malfunctioning components. Company A is under severe pressure to restore normal postal service in major cities, and the CEO has approved recommencing of delivery pods. • The very next day, a few hours into the recommencing of the delivery service using the pods, has led to another incident. The CCS has reported an outage of power, with no visibility or control of the delivery pods. The IT team has now (internally) declared this a potential cyberattack, ceasing all enterprise and supporting IT functions across the entire network at Company A. • A clean up operation to recover the pods has been launched. While no incidents have been reported from any of the other delivery routes, there have been some media reports suggesting traffic has been disrupted in the centre of one of the biggest cities where the pods have steered onto public roads. This has led to panic in the central business districts in the city, where the incidents have occurred, along with early reports of at least one fatality from one of the road accidents due to a pod. Any further disruption is still being established. • Company A's CEO and senior team have convened on an urgent basis to monitor the situation. Both the IT Team and Fleet Operations are investigating the incident, in cooperation with the authorities in the city. The CEO has announced ceasing of all operations, given that all IT networks have been powered down temporarily. The CEO is under pressure from the company board members to hold regular internal briefings.
Scenario 4—'nation–state disruption' (Sc-Nation)
• Following day, the country's national media is reporting a nation-wide cyberattack on critical infrastructure, targeting cellular networks and road traffic management systems in major urban centres including the country's capital and other major cities. Some transport infrastructure (including train stations and airports) that relies on telecommunication systems around the country has also been affected. The attack is affecting power supply to many of these digital systems and assets, directly affecting normal operations. Stations and airports across the country have been put on high alert, with many journeys disrupted due to cancellations. • The country's national cybersecurity agency has approached Company A with a view to conducting a forensic examination across some of the computers, corporate network routers, and control systems interfacing the pod delivery system. The agency staff have confirmed that the impact of the attack on Company A (in Scenario 3) is highly likely to be a source of national disruption; exact details on how the attack propagated from Company A to cellular networks and other national systems is not known however. • More details on the national cyberattack have been released by the media, which point to a vulnerability in the autonomous delivery pods, supplied by the same supplier to Company A. The vulnerability affects the communication and control protocols provided by the supplier to allow for remote teleoperation of the pods. Some of the news reports have even pointed a finger to the attack (in Scenario 3) that targeted Company A, calling it the 'clear source of the attack'. The attack is being attributed to a neighbouring country, which has long been an aggressor to its neighbours. While none of this information has been confirmed by the authorities, this has raised major concerns amongst the top leadership of Company A. • The Board of Directors of Company A are now wanting more details from the IT and Fleet Operations. Some of the Directors are wanting to issue a press release to assure the wider public. All postal operations have been switched to manual operations across the country, even from other postal delivery companies as caution. This has meant a significant effect on postal and logistics nationally, directly affecting the economy.

to complete a presurvey, which included questions to capture their existing risk focus (using the Cambridge Risk Taxonomy).

At the start of the event, there was an introduction session lasting 30 minutes, by the researcher–authors, participants, and the observer. This was especially important given the online format (using a secured Zoom meeting), where we allowed participants to keep their cameras off if they wished. Introductions allowed us to become familiar with who was in the meeting, principally to be able to associate comments to a specific participant when they spoke. One researcher then provided an overview of the research, and demonstrated completion of a 'dummy' survey form.

The four rounds of scenario were each 30 minutes in duration: this time allowed participants to read each scenario once revealed (and kept on-screen) as in Tables 1 and 2, to clarify any content, which was unclear, and to then complete the survey form (as in the Appendix). After reading each scenario, the participants were asked to complete a survey response sheet provided online (see the Appendix for details of these questions). This window of time was also designed to be generous enough as to allow for open discussion of the scenario before moving to the next one. Pertinent participant comments from those discussions were noted by a dedicated note-taker, where these are included to interpret the results from the survey forms as in the next section.

A break was incorporated into the schedule after the first two scenarios, lasting 15 minutes. If any participants needed to 'leave' the workshop while there was still time in each scenario block, they were able to do so. After the four scenario blocks, there was a 30-minute debrief and discussion section, which included overview comments from the observer (who although external to the participating organization, was familiar with them). The workshop lasted 3 hours and 15 minutes, and was attended fully by all participants.

The observer was present during the workshop in the sense of being on the entire online meeting, and making their presence known at intervals. This was in part to assure the participants and maintain an environment of trust. In cooperation with the researchers, the observer kept comments to a minimum during the workshop, so as not to either (i) influence participants' own views, or (ii) disturb the discourse between the authors and the participants. The observer was experienced and knowledgeable in their right, so their input was sought as a closing overview at the end of the debrief. At the end of the workshop, the researchers thanked the participants for their time and closed the event.

Participants

Study participants were recruited from the same organization, brokered by the trusted intermediary and observer (who also attended the workshop event as an observer). Participants represent stakeholders in the organization responsible for decision-making around cybersecurity (and were invited on this basis); this did not include anyone outside of the executive function responsible for implementing any decisions (e.g. IT staff).

As a group, the participants held executive roles in the organization, many of these relating to business continuity, compliance, gover-

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad018/7246580 by Delft University of Technology user on 15 September 2023

Table 3: Scenario dimensions, or characterizations in each scenario.

Characterization	S1 / Sc-Ransom	S2 / Sc-Pods	S3 / Sc-Power	S4 / Sc-Nation
Risk externalities (in terms of who and what is directly and evidently affected beyond the IT Team)	**Who?** • Customers • Staff **What?** • Customer credit card information • Access to company data	**Who?** • Customers • Staff (Fleet Operators) **What?** • Postal Delivery • Staff well-being • Delivery pods • Delivery service	**Who?** • Customers • Company staff (including Fleet Operators) • Public (road users) **What?** • Postal delivery • Life • Delivery pods • Access to IT and digital services • Road traffic disruption	**Who?** • Customers • Company staff • Wider public • Infrastructure owners and operators **What?** • Public life • Postal delivery • Postal services • Telecommunication services • Public transport • Electricity supply
Stakeholder management (internal / external)	• Management • Staff • Legal team • Customers • GDPR regulator	• Management • Staff (including Fleet Operations) • Pod supplier • Legal team	• Management • Staff (all) • Law enforcement (traffic) • Public (loss of life) • Legal team	• Management • Staff (all) • National government • CNI operators • Public (PR) • Legal team
Anticipated risks (in terms of Cambridge Business Risks (family/class) (number of risk families exposed)	• Technology/ cyber/ cloud outage • Technology/ cyber/ data exfiltration • Governance / noncompliance / negligence • Social/brand perception / negative customer experience	• Technology/ cyber/ Internet of Things • Technology/ disruptive technology/ robotics & automation • Governance / noncompliance / occupational health & safety • Governance/ products and services/ innovation (R&D) failure • Financial/ counterparty/ supplier failure	• Technology/ cyber/ Internet of Things • Technology/ disruptive technology/ robotics & automation • Governance/ noncompliance/ negligence • Governance/ litigation/private lawsuit • Social/brand perception/ negative media coverage • Financial / counterparty/ supplier failure	• Technology/ cyber/ Internet of Things • Technology/disruptive technology/robotics & automation • Technology/ critical infrastructure / transport • Technology/ critical infrastructure / power • Technology/ critical infrastructure / telecommunications • Governance / noncompliance / negligence • Governance / litigation • Social/brand perception / negative media coverage • Geopolitical/interstate conflict / asymmetric warfare • Financial / counterparty/supplier failure
Uncertainty factors	• Source and cause of attack • Wider impact of the attack (subject to recoverability), and any 'further damage' that could be caused • Nature of liability to the organization	• Malfunction or link to the ransomware attack • Nature of delays to postal operations • Level of trust in the pod supply chain	• Nature of assessment conducted to reintroduce pods • Cause of power outage • Nature of physical disruption caused by the incident in the city	• Involvement of a nation state • Link between attack on Company A and national disruption (and extent of such disruption) • Content of press release
Responsibility	*5*	*5*	3	1
Att. class.	5 (Moderate incident)	3 (Significant incident)	3 (Significant incident)	1 (National cyber emergency)

The characterizations represent a mix of elements designed into each scenario, and anticipated responses, which would be within expectations when engaging with participants.

nance, and security (Q1 in the presurvey). All participants had over 10 years of work experience, with most (67%) having between 21 and 30 years and one having between 41 and 50 years (Q2).

By capturing information about Direct Reports, we were able to infer that many of the participants in this group work together directly; some reported to others in the group. This may have influenced the discussions (where we saw a few, perhaps more senior individuals leading the discussion, such as PInc1 and PGov5). This was an important artefact of the engagement, potentially emulating a real decision-making hierarchy (among executives) in most large organizations such as this one.

With respect to the summary given by participants of what IT-related decision-making they carry out in their role, replies included mention of cybersecurity awareness, business continuity, compliance, and incident management (Q4). Broadly, PInc1 was responsible for cyber-incident handling and PInc2 with incident response; PCon6, PCon8, and PCon9 are involved in business continuity; PGov4, PGov5, and PGov7 with compliance and governance and PGov3 with

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad018/7246580 by Delft University of Technology user on 15 September 2023

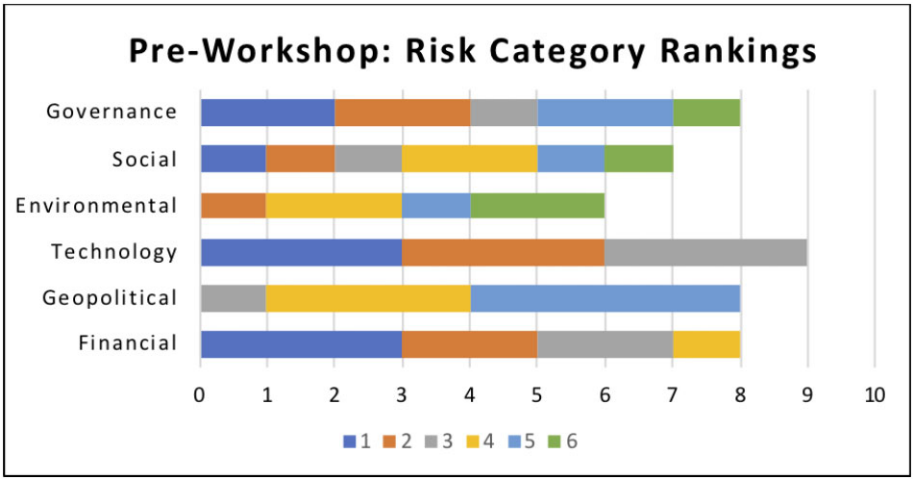

Figure 1: Top perceived cybersecurity risk categories, from the preworkshop survey (1 highest, 6 lowest). The x-axis indicates the total number of participants who have included each category in their ranking.

security awareness. Some of the action verbs commonly used in their summary include: 'Define', 'check/verify', 'manage/handle/monitor', and 'execute'. These may speak to the responsibility of ensuring smooth running of existing security and business continuity frameworks.

Although not strictly a participant, the observer has knowledge of the participating organization. With over 40 years of experience in governance of technology-related risks, the observer provided a credible source of reflection at the end of the exercise, arguably beyond that which the authors could glean from existing research. The presence of the observer served as a bridge between research imperatives and respecting corporate access.

Ethics

The study was approved as part of institutional human-facing research review. This includes satisfying ethical obligations ensuring participatory consent, due governance of data collection (including storage, processing, sharing, and deletion in compliance with GDPR), digital needs met through secure infrastructure, and following distancing protocols due to COVID-19.

We also addressed the principles of the Menlo Report [30] for ethical research in ICT. We did not ask directly for sensitive operational details, and were considerate of the fact that multiple people from the same organization were attending the workshop, encouraging participation where possible while respecting organizational dynamics. We also ensured no hindrance of fair representation of diversity (in terms of age, disability, race, gender, religion, sexual identity) amongst the participants.

We recognized the busy schedules and 'poor reachability' [11] of highly experienced professionals such as our participants: questions were designed to facilitate short answers, and participation was voluntary. The participants were not compensated financially; after the workshop, all participants were provided with a high-level summary report of results and reflections, which emerged from the event.

Results

All of the named authors facilitated the workshop with participants, with two authors speaking to cue participants to read scenario descriptions, complete per-scenario surveys, and to also prompt and lead discussion. Here, we discuss participant responses to the scenarios in initial subsections, as recorded in survey answers, and as also derived from written notes of the workshop (as in the 'Uncertainty and technical complexity' section). We refer to Scenarios 1–4 as S1, S2, S3, and S4, respectively. We note here also that P4 did not complete the forms for S3 and S4.

Prescenario risk ranking

We saw—as in Fig. 1—that not all of the six categories were ranked by the participant group. Rankings also differed and were varied: no category was left not selected and all but Environmental and Geopolitical were ranked first by at least one participant. Technology was prioritized the most, receiving the greatest number of first place rankings, the most selections, and no selections lower than third place ranking. Social received the most varied ranking selections, followed by Governance and then Financial.

We also revisit the broad categories of participant backgrounds as detailed earlier: incident response (PInc1, PInc2), governance (PGov3, PGov4, PGov5, PGov7), and business continuity (PCon6, PCon8, and PCon9). The 'incident response' (PInc#) group prioritized Finance as their top risk where other groups did not; the 'governance' (PGov#) group listed Technology as either their first or second priority area of cybersecurity-related risk; alongside this, the 'business continuity' (PCon#) group was more mixed in their rankings.

Attack categorization and risk ownership

Attack categorizations are shown in Table 4. No participants regarded any of the scenarios as being in categories 5–6, likely as these refer to smaller organizations (which does not apply to this one participating organization). Participants generally saw Sc-Pods as having a more localized impact than Sc-Ransom, even though the 'physical' impact of the scenario events was outside of the organization in public spaces (where more participants noted Social and Environmental risks for Sc-Pods than in Sc-Ransom); this potentially hints at a distinction between escalating cyber-risks and how escalations in noncyber-risks are assessed.

Also, in Fig. 2, Sc-Power and Sc-Nation were given almost an identical classification, even though the context shifted with S3 to S4 from impacts to national postal services to potential nation-level cyberattacks.

When discussing Sc-Ransom after completing the survey, participants noted Company A's role in critical infrastructure, with a nation-wide customer base—the business and potential reputational

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad018/7246580 by Delft University of Technology user on 15 September 2023

Table 4: Number of selections by participants of each attack category (C#).

Scenario	Scen. category	C1	C2	C3	C4	C5	C6
S1	C5	–	4	3	2	–	–
S2	C3	2	1	1	5	–	–
S3	C3	7	–	1	–	–	–
S4	C1	7	1	–	–	–	–

Columns represent the six 'attack classification' categories, category 1 for a much more severe, national cyber emergency, and category 6 for a localized or emergent incident. Rows show category selections for each scenario.

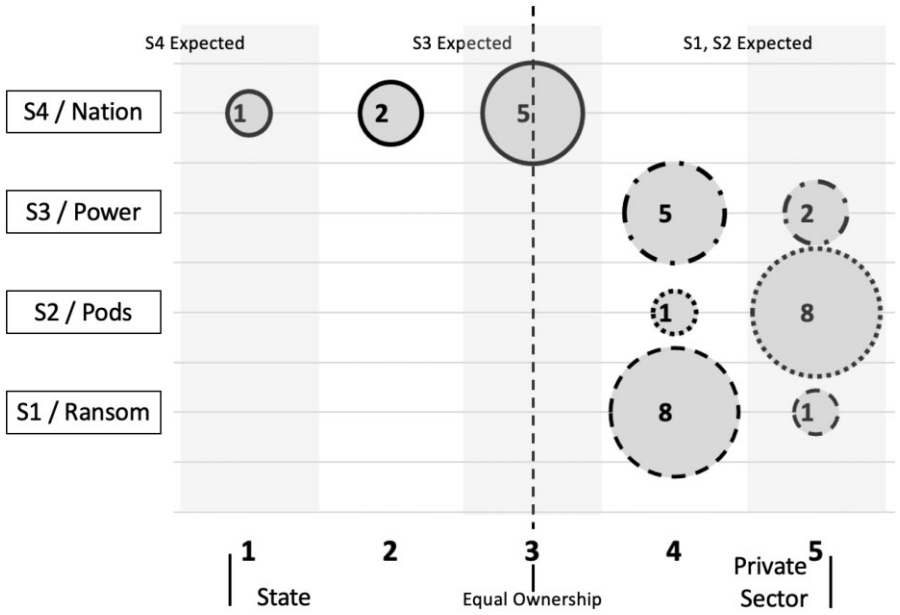

Figure 2: Tally of participant perception of the responsibility of the organization ('private sector') against that of the state in managing the risks in each scenario (S1–S4). The y-axis indicates number of participants who have selected each of the values 1 ('State') to 5 ('Private Sector').

impact was seen as critical compared to the ransomware amount, if Company A is seen as a *'safe harbour'* (PGov5) for (financial) services, for instance. P5 also noted potential legal / data protection ramifications, and P7 the revenue loss from disrupted services (as relates to the higher ranking of Financial). Participants generally pointed to the need to coordinate with national authorities (an element of Governance), where the risk *'extends beyond the organization'* (PGov7).

Sc-Pods: was seen as affecting a limited portion of the organization (PInc1), with options to switch to manual/non-IT activities (PGov3). However, there was also consideration of a potential loss of life (PGov4) though this was limited to injuries (P5). Delays in larger cities (PGov5) account for Environmental and Social impact, with operational risks relating to damage to businesses and to employees (PGov7). The impact on a new business service was also noted (PGov5, PCon8).

Sc-Power: although the risk category selections are comparable to those for Sc-Pods, the attack categorization switches from more of a business-focused issue in Sc-Pods, to S3 being regarded by our participants as a nation-level incident. Participants focused on the *'loss of life'* (PGov3), and that the incident occurred in a major city (PCon6). PGov7 noted that *'The incident is not yet certain, but the impact for Company A is certain'*, noting the social impact, that the reputation for Company A and the technology has been damaged. Different forms of certainty in cybersecurity decisions are noted elsewhere [31].

Regarding Sc-Nation, participants noted a clear national security angle (PCon8), affecting mobile communication (PGov5), transportation (PCon9), and *'high potential for economic and social disruption'* (PGov7).

Participants were asked to indicate their perception of the private–public mix of responsibility for ownership of risks seen in each scenario (Fig. 2), on a scale of 5 (Private sector) to 1 (Public / State). Values around the centre of the scale indicate shared responsibility. What is interesting then is that there is a jump from S1 to S3 (Sc-Ransom, Sc-Pods, and Sc-Power, respectively, being within the private sector, to Sc-Ransom being seen by all participants as including some responsibility for the state—this reflects the nature of the scenario themes. Otherwise, participants clustered their perceptions of responsibility around the private sector / Company A itself. Participants classified the responsibility for Sc-Pods and Sc-Power as in the same region as for Sc-Ransom, even while rating Sc-Pods and Sc-Power as higher types of attack categorization—in discussion, participants made a distinction between managing potential incidents and keeping other stakeholders appraised of them, where the discussion switched around Sc-Nation to being involved at a nation-level.

Scenario risk categorization

For each scenario, participants selected a smaller set of risks than was available (Figs 3, 4, 5, and 6, for scenarios S1–S4, respectively). For the first two scenarios, no participants selected more than four risk categories, reflecting the comparative simplicity of these scenarios.

The selections for Sc-Ransom (S1) are in line with the theme of the scenario, with 'Technology' and 'Financial' risks being selected

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad018/7246580 by Delft University of Technology user on 15 September 2023

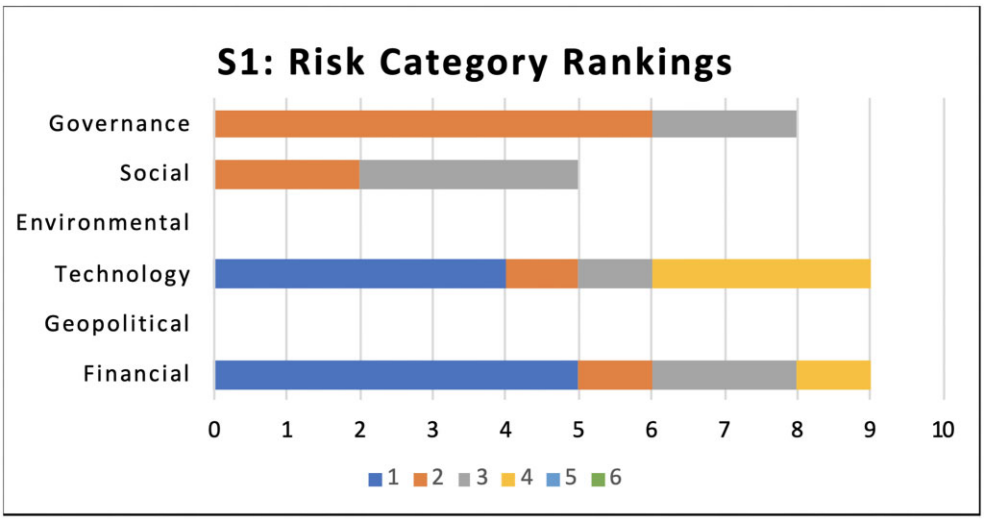

Figure 3: Business risk category rankings by no. of participants, for scenarios S1 (1 highest, 6 lowest). The x-axis indicates the total number of participants who have included each category in their ranking. The legend describes the ranking position (from first to sixth, 1 to 6, respectively). Each distinct block for each of the risk types then represents how many participants selected a particular ranking. As an example, two participants ranked 'Social' risks first for this scenario.

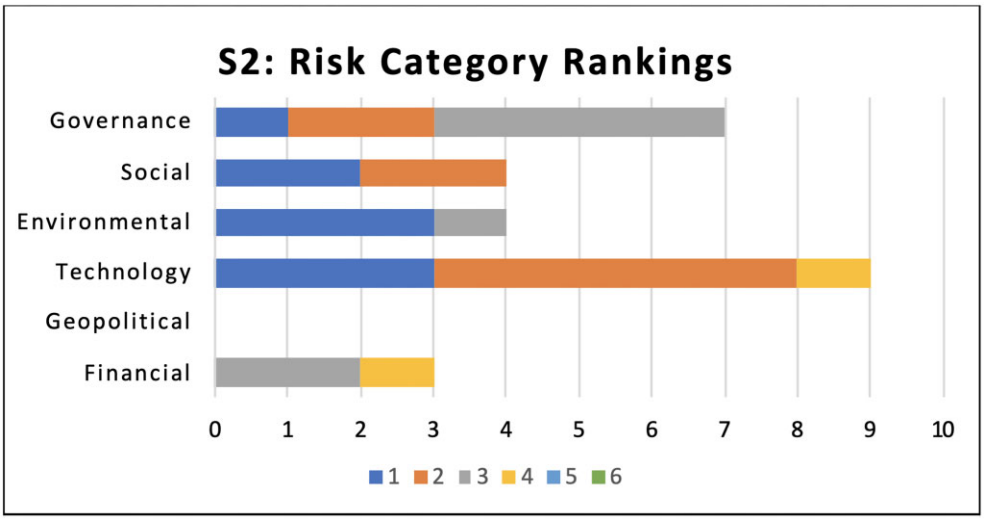

Figure 4: Business risk category rankings by no. of participants, for scenarios S2 (1 highest, 6 lowest). The x-axis indicates the total number of participants who have included each category in their ranking. The legend describes the ranking position (from first to sixth, 1 to 6, respectively). Each distinct block for each of the risk types then represents how many participants selected a particular ranking. As an example, two participants ranked 'Governance' risks second for this scenario, and none ranked it as first.

most. The role of 'Social' risks grew, and 'Financial' risks reduced, with Sc-Pods (S2) and Sc-Power (S3), reflecting their impacts outside of the fictional company. 'Geopolitical' risks did not feature at all for the first three scenarios, but then featured heavily in Sc-Nation (S4), within expectations.

At the end of each round, participants were asked to comment on the scenarios. We report on our findings along with some of the related areas addressed in an open discussion that followed each scenario assessment.

Scenario 1 (Sc-Ransom)

The response noted the due reporting requirements that regimes such as GDPR mandate. This affirmed an understanding of such regulated areas of data and technology. Any such reporting needs to acknowledge associated uncertainties that come with such incidents. Indeed PGov4 acknowledged this explicitly, while PGov7 also emphasized on the need for a *'very prompt assessment of what data has been affected'*, noting both the extent of data impacted and the timeliness of this assessment.

Scenario 2 (Sc-Pods)

The health and safety of the employees was a key concern raised given some of the employees are injured due to delivery pod malfunction. This was linked to potentially a number of risks that may emerge in terms of financial loss, legal action by the regulator, and ultimately governance risks given possible loss of confidence amongst employees (PGov4).

Pertinent to autonomous pods, a key risk noted by PGov7 was the incident leading to a reduction in *'the confidence in a new technology'*. This is often an underplayed area of impact arising out of

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad018/7246580 by Delft University of Technology user on 15 September 2023

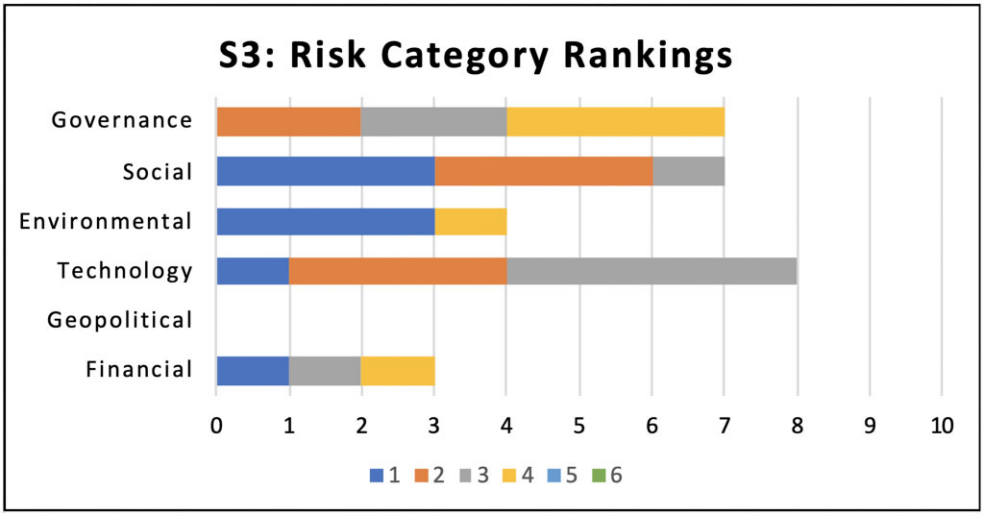

Figure 5: Business risk category rankings by no. of participants, for scenarios S3 (1 highest, 6 lowest). The x-axis indicates the total number of participants who have included each category in their ranking. The legend describes the ranking position (from first to sixth, 1 to 6, respectively). Each distinct block for each of the risk types then represents how many participants selected a particular ranking. As an example, two participants ranked 'Social' risks second for this scenario, and none ranked it as first.

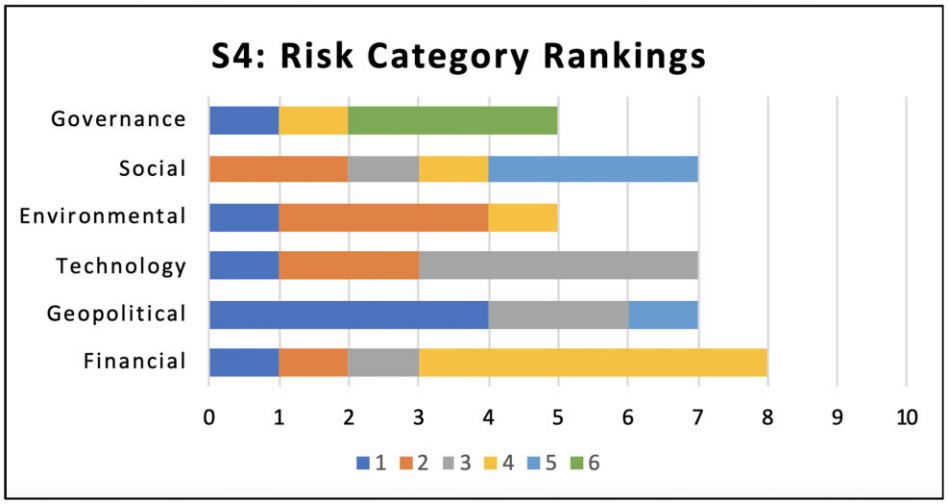

Figure 6: Business risk category rankings by no. of participants, for scenarios S4 (1 highest, 6 lowest). The x-axis indicates the total number of participants who have included each category in their ranking. The legend describes the ranking position (from first to sixth, 1 to 6, respectively). Each distinct block for each of the risk types then represents how many participants selected a particular ranking. As an example, one participant ranked 'Governance' risks as first for this scenario, one ranked it as fourth, and three ranked it as fifth in terms of criticality.

cyberattacks that are now seen to be targeting a number of technology that are only emerging.

Scenario 3 (Sc-Power)

The severity of the incident given the loss of life becomes centre of the attention now. PGov5 confirms this as to say that they classified the event as a level one concern *'because of the fatality that occurred'*, and also noting that in a case such as this *'we have to report to the local authority [...] and also report to the central government'*. PGov7 goes as far as to say that also perhaps *'Parliament would require a question time with the CEO'*.

The focus on the role of the top level organizational leadership is becoming clear now, not only in terms of they have to do but how they ought to be supported, as PGov5 notes *'after taking this advice from the specialist departments, [...] we need all of these specialist divisions to be very close to each other to support [the CEO]'*. This serves to confirm the underlying premise of this research that executive leadership in organizations are increasingly challenged with managing cyber-risks, as an important part of wider business risk management. Acknowledging that such risks are complex, our participants appear to be confirming the role the leadership plays and the support they need.

Scenario 4 (Sc-Nation)

As cyberattacks become major incidents, targeting critical infrastructure and disrupting public life in a substantial way, the risk ownership shifts, as we see in Fig. 2. PGov5 captures this clearly when they say that for Sc-Nation *'the classification is not so uncertain'*, but that in

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad018/7246580 by Delft University of Technology user on 15 September 2023

this case *'the line of responsibility is not clear yet'*, though *'the state is now much more heavily involved in the management of this situation'*. This exemplifies management of different forms of uncertainty at once [31]. PGov5 focuses further on senior leadership, in that *'the board wants to show that it is actively involved and that is in charge [...] it is trying to manage the problem, of course, to investigate it to find the root causes and to solve them'*.

Uncertainty and technical complexity

Our scenarios presented growing uncertainty and technical complexity as they captured an escalating cyberattack.

Uncertainty

Key themes emerging around uncertainty are external stakeholders (which may hold varying levels of relationship with the organization) and impact (as causal links and propagation may not be straightforward). These may be regarded as a mix of unknown and unknowable cybersecurity uncertainties [31].

For Sc-Ransom, PGov7 mentioned the capability to recover data as being uncertain. PCon8 noted that it may not be clear at this point how to resume services.

Around Sc-Pods, there was perceived uncertainty around how the events would be interpreted by employees (PGov4), as it could affect their confidence in being able to work. The reliability in the declaration by the pod manufacturer was also mentioned (PCon9), indicating that external communications are useful for dependent stakeholders to make their own internal assessment of risks.

Regarding Sc-Power, PGov7 noted the main source of uncertainty as determining whether the information on the fatality and traffic disruption is accurate. With Sc-Nation, a concern—again raised by PGov7—was determining whether the vulnerability in Company A facilitated the events in this scenario. These discussions follow a pattern of 'sequential' (or 'joined-up') thinking [31].

Technological complexity

Technological complexity is also a factor towards uncertainty when it comes to establishing causal impact and the full implications of attacks.

For Sc-Ransom, PGov4 raised the question of how we assess the infrastructure impacted, because vulnerability assessment and penetration tests are time-consuming. Somewhat related was how did the attack manifest itself and whether there could be further similar attacks were also questions raised by PGov7 and PCon9.

Across S2–S4 (Sc-Pods, Sc-Power, and Sc-Nation, respectively), participants have similar reactions raising questions that typically arise out of post-mortems of cyberattacks. Attempting to link the ransomware to attacks that followed, PGov3, PGov4, and PCon9 wanted to understand the causal link due to the underlying technical architecture; PGov7 raises this in the context of such attacks impacting national infrastructure.

The use of autonomous pods in the scenarios was deliberate to assess the response against an emerging IoT technology. Only one of the participants (PGov7 in Sc-Power) noted the potentially complex technology underpinning the pods.

Discussion

Here, we reflect on both the design of the scenarios and the responses of participants to the scenarios. In terms of the methodology (RQ1), our use of existing categories of cybersecurity incident severity [29] and business risk [28] guided not only the design of scenarios, but also provided structure to scenario escalation. These categorizations informed the injection of narrative hints around associated risks and externalities, relevant stakeholders, and issues of complexity. Our focus on risk perception and ownership is an acknowledgement that at an executive level decisions are directed at strategy and resource management, where organizational resources can be deployed to overcome risks posed to the organization, and state resources can be invoked where the risk moves on to the wider sphere (that is, to the public and national infrastructure).

Regarding RQ2, our findings show that risks were generally selected within the parameters/expectations in our scenario design (Table 3), though participants noted that local and national governments would be contacted as soon as public spaces were affected (as in Sc-Pods and Sc-Power, and not only Sc-Nation), where attribution of incidents is a critical deliberation that is distinct from communication of information about such incidents [32]. Further, incident task forces would be called into action when the incident was regarded as having become very serious and seen as involving multiple internal and external stakeholders (as with S3 and S4); such crisis teams involve bringing together members of an organization with the skills seen as necessary to improvise a response to an incident [33], such that here convening such a team or committee was seen as an existing approach that was equally applicable to cybersecurity incidents (as noted elsewhere [34]).

The workshop observer provided overview comments after the discussion session. They noted that there needs to be a communication plan for engaging with the media, where this can require careful planning [35]. The observer also commented that in increasingly complex scenarios (noting this particularly for S3), to manage the crisis, there would be a need to understand the causal links between events (which further points to the importance of attribution in cyber-related incidents [32]), where this would typically mean calling on external cybersecurity specialists to conduct an independent review. The observer also indicated that it would be useful to relate risk categories to metrics, in the sense of specific actions being activated depending on specific outcomes, e.g. if there was loss of life or significant loss of money, that it would define the extent to which different levels of crisis committee would meet. PGov7 responded to this, indicating that existing crisis committee procedures would apply well to the events described in our scenarios (so not necessarily requiring a dedicated 'cyber' crisis committee), as they have an organizational perspective and define who is involved in which kinds of crisis.

Our approach could be taken to other sectors where the key aspects that would need adapting would be the scenarios, to ensure thematic relevance to the target audience, and the risk categorization, particularly if the target organization is other than private sector (given our choice of the business risk taxonomy). Public sector organizations, e.g. would have different governance structures to manage resources. Where participating organizations are in the same sector or use similar technologies, a 'bank' of scenarios and scenario components (as described in our scenario design (Table 3) can be constructed over successive engagements, providing potential to meaningfully compare participating organizations.

The design of the approach described here provides options for participants, to fit their views into predetermined scales and categories; this has served well to determine if participants perceive differences between scenarios as they change and escalate according to the dimensions we have integrated into each scenario. In future, the methodology could be adapted to prioritize explanatory mechanisms in the workshop protocol—this could include providing our scenario classifications to participants and asking them to reason as

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad018/7246580 by Delft University of Technology user on 15 September 2023

to whether our classifications fit with their perceptions, or why they do not.

Limitations

Not all participants engaged with the data-collection forms for each scenario, as at least one participant needed to move location between scenario sessions—this was determined in advance and accounted for as best as possible in the workshop (the researchers established availability beforehand, accepting that the participants were making a best-effort to make themselves available all at the same time). Although form completion was not total, most participants did complete the forms consistently for each scenario, and all participants completed the preworkshop form. Senior managers in organizations are a hard-to-reach population, where studies with senior managers should also aim where possible to respect the participants' availability in terms of both attention and time.

Another limitation is that the more senior participants drove much of the open discussion. The dynamics of working culture were considered as an eventuality during the design of the workshop; hence, the moment designed in for each participant to complete the per-scenario forms individually before discussion, as a means to guarantee input from everyone involved.

Ideally, we would have conducted the exercise in-person. The participants were recruited as a group—coming to this group without a prior context, we did not know the interpersonal dynamics. Also, because the workshop was conducted virtually, we had little insightful interaction and cues typical to face-to-face interactions, including any incidental interactions such as a person appearing engaged or confused by anything they are reading. We aimed to compensate for this with the use of the preworkshop survey to gather some context, and the preparatory meeting with the intermediary/observer. We also note that participants engaged with the survey forms and discussion throughout the workshop.

Conclusion and future work

When reflecting on the scenario-based approach, it was noted, for instance by P5, that the escalation of scenarios resulted in a shift of decision-making around risk ownership; P5 further remarked that the last scenario was akin to getting '*to the end of the story*', and that at different stages of progression there would be a different view of (risk) ownership. This is similar to what Shreeve et al. frame as 'complex thinking' in decisions, which returns to earlier assumptions [31]. Future work will explore the potential for the sequence of scenario variations to more explicitly represent an evolving situation and *shifts* in perceived risks, perhaps as one scenario with varying aspects of uncertainty, and the decisions, which participants make in response.

There are initiatives to build capacity in organizations and society to be prepared for broad categories of large-scale risks [6]—these efforts extend to cybersecurity. Regarding 'practices for preparedness', businesses would then prepare themselves to address such challenges by addressing three key capabilities: resilience-by-design, responsibility, and exercise. We have explored the last of these through scenario-driven discussion of preparedness. Discussions also touched on decision-making related to responsibility, and *clarity of risk ownership*. Future work will also include exploration of how scenarios can be used to improve existing preparedness for incidents with a cybersecurity element (where preparedness for situations focused on cybersecurity has been explored elsewhere [31], and here, we consider how decision-making would be impacted by complex and uncertain situations). For instance, pre-prepared playbooks may be practised to respond to specific scenarios (e.g. connected places [36]), where an approach such as ours is an opportunity to develop and rehearse responses to incidents.

Acknowledgements

The authors would like to acknowledge the participants from the partner organization and Richard Knowlton who served as the workshop observer.

Author contributions

Simon Parkin (Conceptualization [equal], Investigation [equal], Methodology [equal], Visualization [equal], Writing – original draft [equal], Writing – review & editing [equal]), Kristen Kuhn (Conceptualization [equal], Data curation [equal], Investigation [equal], Methodology [equal], Writing – original draft [equal]), and Siraj Ahmed Shaikh (Conceptualization [equal], Funding acquisition [equal], Investigation [equal], Methodology [equal], Project administration [equal], Writing – original [equal], Writing – review & editing [equal])

Conflict of interest statement. None declared.

References

1. Shreeve B, Hallett J, Edwards M,. *et al*. The best laid plans or lack thereof: security decision-making of different stakeholder groups. *IEEE Trans Softw Eng* 2020;**48**:1515–28.
2. National Cyber Security Centre. Cyber security toolkit for boards 2019. 2019. Available from https://www.ncsc.gov.uk/collection/board-toolkit (11 August 2023, date last accessed).
3. Greenberg A. The untold story of NotPetya, the most devastating cyberattack in history. 2018. Available from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (11 August 2023, date last accessed).
4. Fiveash K. The Norsk Hydro cyber attack is about money, not war. 2019. Available from https://www.wired.co.uk/article/norsk-hydro-cyber-attack (11 August 2023, date last accessed).
5. Fiveash BBC. Colonial pipeline: US recovers most of ransom, justice department says. 2021. https://www.bbc.com/news/business-57394041 (11 August 2023, date last accessed).
6. Royal Academy of Engineering (UK). Critical capabilities: strengthening UK resilience. 2021. https://raeng.org.uk/media/bm2e4chu/raeng-critical-capabilities.pdf (11 August 2023, date last accessed).
7. Parkin S, Kuhn K, Shaikh SA. Scenario-Driven Assessment of Cyber Risk Perception at the Security Executive Level. In: *Workshop on Usable Security and Privacy (USEC '21)*. 2021.
8. T Stevens, A Ertan, K Floyd ,. *et al*. (eds.). Cyber Threats and NATO 2030: Horizon Scanning and Analysis. NATO Cooperative Cyber Defence Centre of Excellence, 2021.
9. Moore T, Dynes S, Chang FR. Identifying how firms manage cybersecurity investment. *Workshop on the Economics of Information Security (WEIS)*. 2016.
10. Parkin S, Van Moorsel A, Inglesant P,. *et al*. A stealth approach to usable security: helping IT security managers to identify workable security solutions. In: *Proceedings of the 2010 New Security Paradigms Workshop*. Massachusetts: ACM, p. 33–50, 2010.
11. Reinfelder L, Landwirth R, Benenson Z. Security managers are not the enemy either. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. New York: ACM, 2019, p. 1–7.
12. Horne R, Governing cyber security risk: it's time to take it seriously: Seven principles for Boards and Investors. 2017. https://www.pwc.co.uk/cyber-security/assets/governing-cyber-security-risk.pdf (11 August 2023, date last accessed).
13. Nordberg D, Booth R. Evaluating the effectiveness of corporate boards. *Corp Gov* 2019;**19**:372–87.

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad018/7246580 by Delft University of Technology user on 15 September 2023

14. Massie R. Allocating effort: risk and complexity in board directors' engagement with information. Ph.D. thesis, City University London, 2015.
15. Smith D, Elliott D. Exploring the barriers to learning from crisis: Organizational learning and crisis. *Manag Learn* 2007;**38**:519–38. https://doi.org/10.1177/1350507607083205.
16. Hussain A, Kuhn K, Shaikh SA. Games for Cybersecurity Decision-Making. In: X Fang, (ed.). HCI in Games—Second International Conference, HCI-Games 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings. vol. 12211 of Lecture Notes in Computer Science. Switzerland AG: Springer, 2020, p. 411–423.
17. Cyber 9/12 Strategy Challenge. (29 May 2023, date last accessed). https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/cyber-statecraft-initiative/cyber-912/.
18. Atlantic Council. (29 May 2023, date last accessed). https://www.atlanticcouncil.org/.
19. Cyber 9/12 Strategy Challenge. (29 May 2023, date last accessed). https://www.gcsp.ch/.
20. Jalali MS, Siegel M, Madnick S. Decision-making and biases in cybersecurity capability development: evidence from a simulation game experiment. *J Strateg Inf Syst* 2019;**28**:66–82. https://doi.org/10.1016/j.jsis.2018.09.003.
21. Shreeve B, Gralha C, Rashid A,. *et al*. Making sense of the unknown: how managers make cyber security decisions. *ACM Trans Softw Eng Methodol* 2022;**32**:1–33.
22. Rhee HS, Ryu YU, Kim CT. Unrealistic optimism on information security management. *Comput Secur* 2012;**31**:221–2. https://doi.org/10.1016/j.cose.2011.12.001.
23. Merrill N. Security fictions: bridging speculative design and computer security. In: *Proceedings of the 2020 ACM Designing Interactive Systems Conference*. 2020, p. 1727–35.
24. Shapira Z. *Risk Taking: A Managerial Perspective*. New York, US: Russell Sage Foundation, 1995.
25. Heidt M, Gerlach J, Buxmann P. A holistic view on organizational IT security: The influence of contextual aspects during IT security decisions. In: *Proceedings of the 52nd Hawaii International Conference on System Sciences*. 2019, 6145–54.
26. Schechter S. Common pitfalls in writing about security and privacy human subjects experiments, and how to avoid them. *Microsoft* 2013. https://www.microsoft.com/en-us/research/publication/common-pitfalls-in-writing-about-security-and-privacy-human-subjects-experiments-and-how-to-avoid-them/ (11 August 2023, date last accessed).
27. Anderson R, Moore T. The economics of information security. *Science* 2006;**314**:610–3. https://doi.org/10.1126/science.1130992.
28. Cambridge Centre for Risk Studies, University of Cambridge. Cambridge Centre for Risk Studies, 2019; Global Risk Index 2020 Executive Summary. 2019.
29. National Cyber Security Centre. New cyber attack categorisation system to improve UK response to incidents 2018. https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents (11 August 2023, date last accessed).
30. Dittrich D, Kenneally E,. *et al*. The menlo report: ethical principles guiding information and communication technology research. United States: US Department of Homeland Security. 2012.
31. Shreeve B, Hallett J, Edwards M,. *et al*. "So If Mr Blue Head Here Clicks the Link…" risk thinking in cyber security decision making. *ACM Trans Priv Secur* 2020;**24**:1–29.
32. Rid T, Buchanan B. Attributing cyber attacks. *J Strateg Stud* 2015;**38**:4–37. https://doi.org/10.1080/01402390.2014.977382.
33. Kohler JJ, Fragnière E. Crisis team setup for better improvisation. In: *Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference (ESREL2020 PSAM15)*. 2020;1929–36.
34. Fragnière E, Konstantas D, Kohler JJ. On the benefit of mixing varied professional skills to better handle improvisation phases in crisis management: a qualitative survey conducted in Geneva and Valais, Switzerland. In: *2019 4th International Conference on System Reliability and Safety (ICSRS)*. 2019, p. 474–8.
35. Knight R, Nurse JR. A framework for effective corporate communication after cyber security incidents. *Comput Secur* 2020;**99**:102036. https://doi.org/10.1016/j.cose.2020.102036.
36. National Cyber Security Centre (UK). Secure connected places playbook. 2023. https://www.gov.uk/guidance/secure-connected-places-playbook (11 August 2023, date last accessed).

Appendix—participant-facing forms

Pre-exercise questions

1. What is your current role (job title)? [free-text]
2. How many years of work experience do you have? [number]
3. In your current role, who do you report to (given their role/job title)? [free-text]
4. Please give a brief summary of what IT-related decision making you carry out in your role. [free-text]
5. What do you perceive as top cybersecurity risks to organizations? You may choose from any one or more of the following risks: [Financial, Geopolitical, Technology, Environmental, Social, and Governance]. 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). [Six rows, each with risk labels as above].

Scenario questions (x4—repeated for each scenario)

1. Which of the following categories does the incident fall into? Please select only one. [Cyberattack categorization with 'category definition' only]
2. Please explain why you made your specific choice for Question 1. [free-text]
3. Which of the following risk types does this incident raise? You may choose from any one or more of the following listed in the 'Risks' column below. [Financial, Geopolitical, Technology, Environmental, Social, and Governance]. 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). [Six rows, each with risk labels as above]
4. For the purposes of risk mitigation, what is the split of responsibility between the state and the private sector (the organization 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. [5-point scale]
5. From the description of the scenario, what aspects are most uncertain to you, and why? [free-text]
6. From the description of the scenario, what technological areas are most complex to you, and why? [free-text]

Downloaded from https://academic.oup.com/cybersecurity/article/9/1/tyad018/7246580 by Delft University of Technology user on 15 September 2023

© The Author(s) 2023. Published by Oxford University Press. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted reuse, distribution, and reproduction in any medium, provided the original work is properly cited.