Paper accepted for publication in Information Systems Frontiers, 3 February 2025

Being Responsible in Cybersecurity: A multi-layered Perspective

Professor Niki Panteli, Department of Management Science, Lancaster University, Lancaster, United Kingdom. n.panteli1@lancaster.ac.uk

Dr Boineelo R Nthubu, Department of Management Science, Lancaster University, Lancaster, United Kingdom. b.nthubu1@lancaster.ac.uk

Dr Konstantinos Mersinas, Department of Information Security, Royal Holoway University of London, London, United Kingdom. konstantinos.mersinas@rhul.ac.uk

Abstract

The paper posits that in the increasingly connected digital landscape, there is a growing need to examine the scale and scope of responsible cybersecurity. In an exploratory study that involved qualitative interviews with senior cybersecurity professionals, we identify different layers of responsible cybersecurity that span across techno-centric, human-centric, organizational (intra and inter) and societal centric perspectives. We present these in an onion-shaped framework and show that collectively these diverse perspectives highlight the linked responsibilities of different stakeholders both within and beyond the organization. The study also finds that senior leadership plays a crucial role in fostering responsible cybersecurity across the different layers. Implications for research and practice are discussed.

Keywords Cybersecurity, Responsible, Digital Responsibility, Exploratory Study, Onion-Shaped Framework, Leadership

Introduction

With expanding digitalization, due to but not limited to a growing dependence on cloud computing and the popularity of hybrid work, as well as increased inter-connectivity within and between organizations, maintaining robust cybersecurity becomes a necessity. This is a time when cybersecurity attacks are becoming increasingly prominent and widespread and are a constant threat to individuals, organizations, and societies at large. At the same time there is a growing awareness of the potential cybersecurity harms, and the risks involved. Cybersecurity incidents do not just cause unnecessary disruptions to organizations and their business operations, but they also lead to huge financial and reputational costs to the organizations involved (Safa et al., 2016), and society more widely (Agrafiotis et al. 2018). Within increasing recognition of these wider implications of cybersecurity threats and attacks, calls have been made for the study of cybersecurity to develop rigorous foundations derived from the integration of innovative managerial, technological and strategic solutions (Choo et al. 2022).

Against this background that encompasses multiple, diverse and networked stakeholders, both internal and external to the organization, we posit for the need to develop an understanding of cybersecurity from a responsible perspective. Such perspective is known to facilitate co-creation and engagement with diverse stakeholders whilst it has the potential to nurture the generation of shared value that results in increased benefits for all stakeholders involved (Pappas et al. 2023). The need for responsible cybersecurity, both in terms of understanding its scale and scope, and also in terms of promoting it, stems from an increased realization that cyberthreats and attacks have implications beyond single organizations and the individuals within them, to entire sectors and societies at large.

There has recently been a rising interest in *responsible digital*, with the focus on AI attracting most of the attention in this space (e.g. Mikalef et al. 2022; Trocin et al. 2023). Nevertheless, responsible cybersecurity remains largely unexplored. Yet, considering the far-reaching implications of cyberattacks, it is important to consider whether the design, use, and governance of cybersecurity systems (with systems used broadly to cover technology, people and processes) is responsible. Following these, the driving questions of this study are:

What is the scale and scope of responsible cybersecurity? And how can organizations foster responsible cybersecurity?

The study draws on an exploratory qualitative study with semi-structured interviews with senior cybersecurity professionals. Based on our findings, responsible cybersecurity is viewed as a *collective commitment where multiple stakeholders act as stewards, not only of their own data, but also of their supply chain and the broader well-being and care of individuals and society*. Findings highlight five core layers of responsibility: **techno-centric**, focusing on technological defenses; **human-centric**, emphasizing security solutions designed with users in mind and safeguarding the well-being of security professionals and other organizational members; **intra-organizational**, stressing the role of team collaboration and leadership buy-in in promoting a positive security culture; inter-**organizational**, concerning the security of supply chains and third-party partners; and **societal**, recognizing the implications of security solutions on a broader societal scale. This multi-layered approach emphasizes that cybersecurity is not just a technical problem that should be left in the hands of cybersecurity professionals, but a collaborative effort among diverse stakeholders at different levels.

Drawing on these findings, the paper contributes to the literature by developing an onion-shaped framework of responsible cybersecurity, on the one hand showing the boundaries of responsibility, and on the other hand, the extent of responsibility with the involvement of

multiple stakeholders within each of the layers. The study argues that the layers are connected and that senior leaders play a key role in developing their connections. Further, the study advances the field of responsible digital by integrating different and diverse perspectives of responsibility, whilst capturing a broad base of individuals within and beyond the organization. A third contribution is in the area of leadership with senior leaders found to be the vectors for the multi-layered responsible cybersecurity.

In what follows, we review relevant literature on responsible digital and cybersecurity as a way for developing the conceptual foundations of the study. Following this, we present the research design and methodology of the empirical study, and the analytical approach adopted. We then present the findings which lead to the development of a theoretical framework on responsible cybersecurity.

The Responsible Perspective: A Growing Trend and its Significance

With the discourse on digital innovation predominantly emphasizing the enormous capabilities of emerging technologies on organizations and society, a responsible perspective is said to bring a more balanced approach to dealing with the challenges of digitalization (Zamani et al., 2023) but also managing grand societal challenges such as inclusivity and sustainability (Voegtlin et al., 2022).

Literature on responsible digital technologies has discussed ethical challenges such as bias reinforcement, lack of transparency and the need for regulation (Trocin et al., 2023). As such, advocates of responsible digital and digital responsibility have argued for the need of ethical, human, and social values to be central within the design, adoption and use of digital innovation (Van de Hoven, 2013; Ahuja et al., 2023). For example, Zhang and Hon (2020) refer to digital responsibility as the ethical and accountable use of digital technologies and includes ethical

decision making, online behavior, and protecting one's privacy and security. Several reasons have been cited for responsible digital. When digital technologies are designed, implemented and used based on responsible principles, they promote fairness and equality (Trocin et al., 2023) whilst also limit, and even avoid, dramatic negative consequences on human and societal well-being (Dignum, 2019).

With specific reference to responsible digital transformation, Pappas et al. (2023) argue that digital initiatives need to be designed and implemented in a way that benefits multiple stakeholders. They posit that the value of such digital initiatives should be both co-created and shared. According to these researchers, responsible digital is a process of integrating digital technology into a business in a way that is 'ethical, sustainable, and respectful of human values and society' (Pappas et al., 2023). The expectation is that when digital (and other) initiatives are built on responsible principles negative outcomes are avoided, whilst individuals, organizations, and societies experience significant positive impacts (Dignum, 2019).

Early attempts to identify *responsible* principles have derived from the Corporate Social Responsibility (CSR) agenda and Responsible Innovation (RI) literature. According to the CSR literature, organizations have a responsibility to contribute towards beneficial impacts to the wider society including economic, legal, ethical, and philanthropic (Carroll, 1991). Under the condition of increased globalization and increased social challenges, calls have been made for a politicized corporate responsibility with an embedded responsible governance structure to ensure the allocation of value created (both economic and social) to diverse stakeholders (Bacq & Aguilera, 2022; Scherer & Palazzo, 2011). The acceleration of digital transformation has expanded this agenda, leading to calls for corporate digital responsibility (Mihale-Wilson, 2022).

Taking a narrower focus on the innovation practices of organizations, RI entails a body of literature that considers responsible at the societal level; the position taken is that there is a need to align research and innovation with societal needs (indicatively, Owen & Pansera, 2019; Stahl, 2022). RI has been broadly defined as a collaborative and interactive process between innovators and societal actors in order to contribute to innovations that are sustainable, and which have social and ethical acceptability (von Schomberg & Hankins, 2019).

More recently, advancements in artificial intelligence (AI) and generative AI have contributed to an almost urgent call for responsible digital. The latter has been conceptualized in the Information Systems domain as ‘a set of principles that ensure ethical, transparent, and accountable use of AI technologies consistent with user expectations, organizational values, and societal laws and norms’ (Mikalef et al., 2022), and as ‘the practice of developing, using and governing AI in a human-centered way to ensure that AI is worthy of being trusted and adheres to fundamental human values’ (Vassilakopoulou et al., 2022). Studies exist on responsible AI in specific sectors and with more calls to compare responsible AI across different sectors (e.g. Barello et al., 2016; Reddy et al., 2019; Wang et al., 2020) and to identify the constituents of responsible AI. For example, Kumar et al. (2023) examine responsible AI in healthcare and find that there are three underlying dimensions: technical skills, ethical concerns, and risk-mitigation. In their empirical study they also find that responsible AI is influenced by data and algorithmic issues, privacy invasion, adaptability, quick recovery from malfunctions, and the extent of collaborative efforts.

Drawing on the diverse responsible perspective literature, the consensus is that multiple stakeholders should be considered when designing, developing, and implementing responsible

initiatives. With our study, we seek to add to this body of literature by examining the case for a responsible perspective within the cybersecurity field.

Cybersecurity: A Need For A Responsible Perspective

If we consider a brief historical evolution of cybersecurity, or information security, we see its initial roots limited to cryptography and mathematics (Schneier, 2015). The nature of cybersecurity has since been transformed into being more pervasive, spanning from people's everyday lives and activities, to groups, organizations, and ultimately to society. Accordingly, the scope of responsibility in relation to cybersecurity has expanded significantly.

The increasing inter-connectivity and reliance on digital technologies, the Internet-of-Things (IoT), and the billions of devices globally, ranging from household gadgets to industrial machinery and to critical infrastructure, constitute a vast digital environment. This environment has an expanding *attack surface* due to the complexity introduced by connecting diverse platforms and new technologies (Dimitrov, 2020), introducing risk allowing for the creation of externalities and network effects, by which compromising the security of one entity affects the overall security of the broader network. Malware on a single employee device, e.g., cultivated under bring-you-own-device (BYOD) policies, can compromise the security of the whole organization. In this spirit, responsibility, as a key component of security culture, refers to the involvement, agency, and ownership of users with regards to the security of the organization (Carpenter & Roer, 2022). This is a bilateral relationship, from employees to the group, and vice versa, and one which allows for the shaping of collective values, beliefs, and attitudes that directly influence security behavior and the overall security posture of the organization. Then, supply chains tend to be globalized, with significant numbers of third parties for each entity in the chain, across geographic locations and platforms. Supply chain compromises are estimated

to account for between 17% to 62% of the total intrusions in 2021 (ENISA, 2022). Cloud computing, then, has introduced additional security challenges for data in transit and data at rest, with additional denial-of-service risks.

These issues are not new in cybersecurity; third-party risk management has been a well-known serious and difficult-to-solve problem within supply chains (Pandey et al., 2020). It is not a surprise that organizations are investing heavily in advanced threat detection and response systems (Sewak et al., 2023) as a way for dealing with the challenges of digital inter-connectivity. However, the scope of *responsible cybersecurity* requires a broader perspective. For example, there is a need to consider employees' needs and emotional well-being at a time of increasing cyber threats and attacks on organizations. The impact on employees suffering a security breach, either targeted to personal or organizational data and services, can be hugely damaging (Wheatley et al., 2016). Moreover, cybersecurity is not limited to organizations' employees and end-users but essentially relates to every individual in digitally advanced societies. A privacy violation of a single individual's personal data can have devastating effects for the well-being of that person (Durnell et al., 2020) and potentially their wider social network; a leak of confidential information or a denial of service due to a ransomware attack can have catastrophic consequences for a company and its employees; then, the exploitation of a vulnerability in any of the healthcare, transportation, energy, financial etc. sectors can have devastating societal impacts. Based on the above, the need for a holistic perspective on the scope of responsible cybersecurity becomes clear. We explore this need through our empirical study which we present below.

Research Design and Methodology

For this exploratory study, we invited cyber leaders, e.g., Chief Information Security Officers (CISOs) and related roles, as well as cybersecurity consultants and other professionals across a range of organizations and sectors to take part. In particular, we conducted semi-structured interviews to explore understandings and attributes of responsible cybersecurity, and the role of the organization and cyber leaders in promoting this cybersecurity perspective. Through their participation in the study, interviewees were encouraged to share their understanding of responsible cybersecurity and contribute towards the co-design of a framework for fostering a responsible cybersecurity mindset. Our interview protocol consists of questions such as: *How would you define responsible cybersecurity? In your view, what are the fundamental principles (dimensions) that responsible cybersecurity should encompass? What challenges does your organization face in adhering to the fundamental principles of responsible cybersecurity? Are there specific opportunities or best practices that contribute to fostering a responsible cybersecurity approach?* These questions were designed to prompt participants to reflect on their experiences and articulate the attributes of responsible cybersecurity, which then informed how responsible cybersecurity can be fostered moving forward. This data generation strategy yielded diverse perspectives on responsible cybersecurity as seen through the eyes of cyber leaders, aligning with best practices in interview design to generate rich data, as discussed in Schultze and Avital (2011).

Following ethical approval (LU 2024-4329-RECR-3), participants were recruited using purposeful sampling to ensure that those selected had direct cybersecurity experience. The inclusion criteria required participants to be in a leadership role specifically within cybersecurity, such as a Director or CISO, or to hold a position that involves leading cybersecurity initiatives. Invitations were distributed through cybersecurity groups,

cybersecurity incubators, university executive program networks, and our own professional connections to reach individuals with relevant expertise. We further employed snowball sampling (Myers and Newman, 2007), to expand our participant pool and reach data saturation.

We began data collection by piloting our interview schedule with 3 participants. This process enabled us to refine the design of our interview questions (Young et al., 2018). In total, 20 interviews were conducted in the period between May and August 2024 and included 15 male and 5 female participants. While efforts were made to achieve a balanced gender representation through efforts to recruit more women, the participant pool ultimately reflected the lack of diversity in the field (Branley-Bell et al. 2022; World Economic Forum, 2022). Our participants represent a range of sectors including finance, IT, transport, consultancy and government. Their experience in the cybersecurity sector varies from 5 to 30 years (average of 16.75). The duration of the interviews which took place online (via Teams) was between 25 to 70 minutes (average of 54 minutes) and they were all audio-recorded and transcribed. Participants were invited to the study until data saturation was reached, stopping when no new insights emerge (Saunders et al., 2018). Table 1 presents the participants' demographics.

Table 1: Participants' demographics.

Participant	Gender	Role	Sector	Years in Industry
1	M	Director, Security Operations	Telecommunication	>10
2	F	Director, Higher Education	Cybersecurity academy	>10
3	F	Senior Cybersecurity & Data Protection Advisor	Digital services and consulting	>30
4	M	Head of Cyber and Security Engineering in Digital Channels	Financial services	>10
5	M	Director of Security for Manufacturing, Utilities & Services	ICT	>20
6	M	Head of Cyber and Innovation	Law enforcement	>5
7	M	Infrastructure Architect	Aviation & transport	>30
8	M	Applications Architect	Aviation & transport	>5

9	M	Chief Information Security Officer	Financial services	>18
10	M	Cyber Security Manager	Public finance and accountancy charity	>16
11	M	Head of IT	Higher education	10
12	M	Technical Manager	Higher education	>5
13	F	Director	Cybersecurity	>12
14	F	Director	Cybersecurity	>24
15	M	Director, Digital Convergence & Information Systems	Transport	>25
16	M	Head of Third-Party Assessments	Financial services	>16
17	M	Board Member	Cybersecurity & computer forensics	>30
18	M	Product Director, IT Security	IT & consultancy	>16
19	F	Director, IT	Food	>12
20	M	IT Security teacher	Education & technology	>31

Analytical Approach

An inductive qualitative analytical approach was adopted with the aim to explore the meaning, scale, and scope of responsible cybersecurity. NVivo was used for the organization and retrieval of data (Mortelmans, 2019) and analysis was informed by Gioia et al., (2013) and Gioia (2021). This approach enabled us to develop the definition and framework of responsible cybersecurity from participants' raw statements rather than from pre-existing theories or hypotheses (Gioia et al., 2013). For this analysis, all the transcripts were read line by line by the second author noting key terms used by participants for defining responsible cybersecurity, key responsible dimensions and effective ways for fostering responsible cybersecurity deploying these as open codes. In this first order coding, terms used by participants such as "*well-being*", "*stewardship*", and "*top-down approach*" were retained, resulting in 57 first-order categories emerging from the data. This step ensured that codes were developed

inductively from empirical data to enable the discovery and theorization of new concepts associated with responsible cybersecurity (Gioia, 2013).

Following the first-order coding, the 57 categories were examined for conceptual similarities and differences and grouped resulting in a reduction of categories to 24. In this second-order category analysis, categories were labelled using participants' terms such as: "*shared responsibility", "responsible use", "secure by design", "ethical by design", "security of the supply chain",* and *"leadership support".* This phase focused on identifying key concepts that capture the meaning of responsible cybersecurity, e.g. "*stewardship*" and "*shared responsibility*." Concepts contributing to the dimensions of responsible cybersecurity, such as "*inclusivity and diversity*," "*well-being*," and "*ethical awareness*," were also identified, Additionally, concepts such as "*supply chain security*", and "*public security*" were identified capturing the scale of responsibilities.

In the next step, the 24 categories were clustered into 7 aggregate themes following extensive discussions among all authors. The first theme relates to defining responsible cybersecurity, we labelled this theme s*tewardship and shared responsibilities* retaining the terms used by participants to define responsible cybersecurity. The next five themes were interpreted as encompassing both the scope and scale of responsibilities and were labelled as *techno-centric, human-centric, intra-organizational=centric, inter-organizational-centric, and societal centric perspectives.* The last theme represents effective leadership practices that foster responsible cybersecurity, contributing to *leadership* as another aggregate dimension. Table 2 presents the data structure as a graphic depiction of how the analysis evolved from raw participant terms through second-order category to aggregate dimensions.

As recommended in Gioia (2021), we utilized the data structure to develop the theoretical framework of the study. In our study this is presented as an "*Onion-shaped Responsible*

Cybersecurity Framework" model that describes what we theorized as "*the multiple layers of responsible cybersecurity*" where each layer encompasses the scale and scope of responsibilities that broaden with each layer. Further, we utilized the data structure to develop a graphical representation of this model, presented in Figure 1. Next, we went back and forth between the codes and the data to refine the links between the layers. This led to the identification of key leadership practices as vectors for the inter-connections between the layers (Table 3). The last step involved utilizing the data structure, the responsible cybersecurity framework, the layer inter-connections, and the leadership practices to present our findings on the definition of responsible cybersecurity, a responsible cybersecurity framework, and the leadership best practices for fostering responsible cybersecurity.

Table 2: Final data structure for themes in responsible cybersecurity dimensions.

First-order coding	**Second-order coding**	**Aggregate dimensions**
Well-being of people	Caring for people and data	Stewardship and shared responsibilities
Protection of data		
Responsibilities to others beyond the organization	Shared responsibility	
Everybody's responsibility		
Stewardship	Stewardship	
Ethical dimension	Ethical aspect of security	
Secure software development	Secure by design	Techno-centric
Designing secure processes		
Access management		
Awareness of AI harm while also harnessing its opportunities	AI security	
Dedicated technical team	Technical capabilities	
Neuro inclusion	Inclusivity and diversity	Human-centric
Managing neurodivergent teams		
Increasing female representation		
Cybersecurity professional's well-being	Well-being	
Stress among cybersecurity professionals		
Burnout among cybersecurity professionals		
The health of cybersecurity professionals		

Psychological safety		
Usability	User-centric-security systems	
Responsible technology use	Responsible use	
Individual security		
Robust security culture	Organizational culture and behavior	Intra-organizational
Awareness training		
Shared responsibility	Collaborative approach	
Collaboration		
Personalised solutions		
Context-specific security		
Data protection	Risk and compliance	
Risk management		
Agile policies		
Supply chain risks	Supply chain security	Inter-organizational
Ecosystem risks		
Spread impact		
Stewards of other's data	Stewardship	
Responsibilities to one another		
Ethical implication of software development	Ethical by design	Societal-centric
Ethical implication of actions and behaviors	Ethical awareness	
Ethical side of work		
Intentions behind software development		
Public security	Public security	
Sustainability	Sustainability	
Top-down approach	Leadership support	Leadership
Sponsorship and funding		
Leadership buy-in and commitment		
Lead the mindset change	Lead change	
Foster a culture of awareness and accountability	Foster a cybersecurity-aware culture	
Role model the values and ethical dimension of security work	Promotion of the ethical dimension of security	

Findings

Responsible cybersecurity has been described by study participants as a form of stewardship depicting a practice as well as a commitment to being ethical and accountable: "*if we consider*

ourselves to be stewards of other people's information, other people's services so then we have responsibilities as stewards." (P17)

There is consensus that this stewardship does not fall within any particular individual but is a shared responsibility. According to a participant: "*Responsible cybersecurity involves assigning responsibilities to individuals, organizations, and regulatory bodies to ensure the protection and proper functioning of systems across all sectors, managing risks and safeguarding against emerging threats like AI misuse." (P15)*

Further to this, our analysis reveals that responsible cybersecurity is understood through the lens of the different stakeholders involved and who may be impacted by potential harms:

"*Responsible cybersecurity for a company involves balancing the security of the organization with the rights and interests of its individuals, ensuring that decisions made to protect the company do not inadvertently compromise the security or well-being of its employees or the broader environment." (P18)*

From the above, different perspectives of responsible cybersecurity evolve, notably techno-centric, human-centric, intra-organizational-centric, inter-organizational centric, and societal-centric perspectives. In the following sections we present each perspective in detail, exploring their unique contributions to responsible cybersecurity.

Techno-centric Perspective

The techno-centric perspective serves as the foundational aspect of responsible cybersecurity. This layer emphasizes the fundamental responsibilities when safeguarding information systems, drawing on the principles of security by design, leveraging AI security, and engaging a competent cybersecurity team to spearhead the cybersecurity mandate. According to participants, the key responsibility in the technocentric layer is ensuring that systems are secure

by design, a recognized view within the literature that advocates for security to be integrated into the design phase of systems and software, rather than being added as an afterthought (Duncan, 2020). This approach ensures that security considerations are embedded in every layer of development, from architecture to deployment:

> *"It can be the responsibility of the people who are developing software and services, that they make sure their services are secure, that they put that kind of thought into it initially, ensuring that the right safety measures and safeguards are there for companies or other people coming to use their services." (P6)*

Participants consistently emphasized that a specialized group of professionals who are responsible for implementing and overseeing the technical aspects of cybersecurity is a responsible matter for every organization:

> "*There needs to be somebody responsible for information security. There needs to be somebody that is paid to be the Information Security Manager, the CISO so to be able to and …have the mandate to do stuff like this.*" *(P3)*

However, the implementation of this responsibility can be resource-intensive requiring the necessary financial support.

Further, while a security-by-design approach may offer robust defenses, it also presents challenges in terms of usability. Therefore, though secure systems and protocols may provide robust protection in technical terms, the effectiveness of these measures can be significantly undermined if the human factors are not adequately addressed:

> "*…, you should not rely only on protective measures but should make* sure *these users* are *aware that they are part of the security ecosystem. So, the involvement of the users is really critical. And the human factor is the one that is going to seem to fail because*

systems are designed by special manufacturers who know what to protect and they're updated regularly. So, it is not easy to bypass the system. And this is well known to the hackers as well. So they prefer to exploit gaps they can identify in their communication with the users rather than spending time in bypassing the security structure of a system. Cyber security is related. I cannot find the percentage to *say how much is directed to the user responsibility and how much to the system. But I can say that a lot of discussion is going on about how to make the users aware, so you have to implement training." (*P15*)*

This last statement indicates that responsible cybersecurity requires a union of secured systems and the responsible use by users, hence the next perspective which focuses on the responsibilities to people and on user's responsible use of technology.

Human-centric Perspective

The second perspective of responsible cybersecurity focuses on human factors. We call this the human-centric responsible perspective. Findings point to two aspects of the human-centric perspective. First, it encompasses fostering *responsible use* and *individual security* through recognizing diverse behaviors, the risks they may present, and creating more targeted and *inclusive* awareness programs. Promoting responsible use also necessitates considering user's needs in terms of usability and finding a balance between security and usability. User *centric-security systems* support responsible use as users can bypass difficult to use systems leading to security risks: *"Security starts with the individual. Because anything you do within security can be undone by individuals, so individuals have got to understand their responsibilities." (P18)*

"I have a responsibility to make sure that whatever procedures I put into place, whether it's two factor authentication or whatever, is usable, it makes sense in their [employees] job, in their context, because ultimately, then it will make the whole system work better." (P2)

Second, our findings show that human factors in cybersecurity extend beyond the individual responsible use of technology. They encompass the responsibility towards the *well-being* of those in cybersecurity roles to ensure they are supported mentally and physically to sustain their effectiveness in a high-pressure environment and to avoid risk behaviors that could be presented due to burnout and fatigue. This issue emerged from our data as a significant finding due to the high levels of stress, burnout, and poor mental health reported by our participants:

"Health-wise, because cyber security professionals, it is expected that at any point in time, they should be able to respond. That's why we have the security Operation Center which we monitor security events 24/7. If there's anything we should be able to respond. ...due to that then it compromises the health (of security professionals) because you are always needed 24/7." (P9)

These findings highlight the need for organizations to support well-being initiatives, foster a culture that prioritizes work-life balance, and provide access to health interventions, ensuring that cybersecurity professionals can perform at their best without compromising their health: *"You are responsible because you are putting in tools and processes in place that helps your staff [cybersecurity team] deliver the best possible service, but also keeping them not mentally challenged and not overstressed." (P7)*

"Ensuring the well-being of people working in the industry ...you want to be a responsible supplier partner, but to achieve that you need to be considering your workforce." (P5)

Also highlighted as important is the need to diversify and to be more inclusive by appropriately managing neurodiverse teams, and increasing women representation in cybersecurity:

> *"we know through an IPSOS survey that happened last year that there's a higher proportion of neurodivergent people in cybersecurity compared to other industries. ... actually 20% of the population is neuro divergent. .... Whether that they have dyslexic dyslexia, dyspraxia, ADHD, autism, and all the other intersectionalities So actually, if you cater for these differences at the start of, you know, maybe the recruitment process then you will have a more inclusive company anyway," P13*

> *"from the point of view from gender diversity, we need to focus and to bring more women in (cybersecurity)." P4*

The human-centric perspective with its emphasis on training and looking after employees has links with the next perspective, i.e., the intra-organizational perspective.

Intra-organizational – centric Perspective

The third perspective of responsible cybersecurity centers around organizational factors and we present this as the intra-organizational centric perspective. This perspective is seen by our participants as a systematic approach to protecting data and people by developing a strong security culture and embracing shared responsibilities among all stakeholders: *"There needs to be the culture in place and it needs to come from top-down." (P3)*

Our analysis highlights the need for a shift in mindset from viewing security as solely an IT problem towards promoting responsibility at the organizational level. In doing so, it is possible to embrace a sense of *collective responsibility*, where all different functional areas, departments and teams prioritize cybersecurity and actively work to reduce cyber risks within their areas of

work: *"Responsible cybersecurity is everybody within the organization and everybody has to acknowledge and understand that they have a role to play." (P10)*

"Everyone has got a hand in it. It is everyone's responsibility." (P7)

This mindset shift necessitates a *collaborative and inclusive approach*, where departments work closely with the security team to develop tailored solutions that meet their specific needs.

A collaborative mindset is also crucial for bridging the gap between the differing mindset on cybersecurity that may exist within different parts of the organization. Participants highlight that business (non-IT) teams frequently perceive the cybersecurity team as policing or obstructing business operations, leading to disconnects and tensions:

"People see security as slowing them down and limiting them." (P10)

"We have got mindsets that, like the service security mindset, which is always looking at things going wrong. I find that quite common within the cybersecurity industry itself. Then you have got the supposed entrepreneurial business mindset, which takes risks, but assume that things are going to go right because they are going to make money out of this. So, there are different views of things stopping things going wrong, having things going right, and these sort of cultures." (P17)

"The security team is seen by others as, let's say a Police Department." (P4)

"Cybersecurity is seen as a technological issue, and it is for IT to solve and, me sat in HR or finance, cybersecurity, I am not responsible for that type of thing. Where really, not really, cybersecurity is everybody's responsibility. So to me, that is what responsible cybersecurity sort of says to me." (P10)

A collaborative approach promotes finding common ground between the cybersecurity team and other departments, especially where teams tend to work in silos as reported by our participants. This can be achieved by establishing a culture that fosters collaboration, bridges the gap between business and security teams, and shifts the perception of cybersecurity from a niche IT problem to a shared responsibility impacting everyone. Further, viewing cybersecurity as a collective risk management challenge empowers individuals to take ownership of reducing risks within their roles, projects, and departments:

> *"… All parts of the business now feed into a cybersecurity risk ...It is ensuring that, it is not a technical implementation. It is ensuring that everyone is part of cybersecurity, works towards this, whether that's someone is in facilities etc." (P11)*

Further to developing a collective and collaborative mindset towards responsible cybersecurity, several practical approaches were mentioned by participants. For example, promoting training and awareness programs are indicated as a crucial way to foster responsible cybersecurity: *"You need to have security awareness program that target different age groups, different genres? You cannot have a one-size fits all." (P1)*

Additionally, implementing agile policies that encourage responsible use and establishing accountability structures to ensure that those responsible for cybersecurity uphold their obligations is equally vital: *"The rate at which things are evolving, you need a more agile approach to policy development." (P1)*

> *"Challenge is not having proper policies, proper security policies, procedures, guidelines. And then again, the accountability if the accountability is not there. If the monitoring is not there, then it is then it's going to be difficult to do anything." (P12)*

Compliance to legislations was seen by participants as a way that companies are being made to care:

> *"Ideally where we want to be is that people are compliant not simply to be compliant, but because it's a way that we manage our obligations towards others and to ourselves. ...So, for example, GDPR isn't simply something to be compliant to, it's a way that society tries to say you have responsibilities towards the privacy of others." (P17)*

There was greater emphasis on the notion of going "*beyond regulations*". In a sense that being compliant does not make an organization responsible but rather as a result of exercising responsibility towards each other. An example from one of participants highlight how this is practiced in their organization:

> *"Another part of being responsible is that you should know what you need to do over and above what your regulator is asking you to do, because what the regulator is asking us to do may not be relevant to the type of threats that we are seeing. For example, for aviation, we had to first self-assess ourselves to see where we stand against the requirements that were dictated or mandated, and then what were the gaps between what was expected versus where we were?" (P8)*

The remaining perspectives are found to extend beyond the boundaries of the organization and include organizational as well as societal:

> "*The problem is not only with you, because if you create a paradise security-wise, you operate in a market, I mean you have connected your systems to other providers or customers. If your providers* or *your suppliers have not made the certain steps to secure their systems, then there will be* [an attack] *from outside so you might have a completely secure system, but if you collaborate with another supplier that is* not *secure*, then *you have a problem because security affects the whole supply chain.*" *(P15)*

This statement highlights that the security of an organization is not an independent matter, but rather, it is inter-connected and inter-dependent on the security of others within their supply chain. We present this inter-dependency in detail in the next perspective which we term inter-organizational perspective.

Inter-organizational -centric Perspective

The inter-organizational perspective emphasizes the inter-connectedness of an organization's cybersecurity with the security of other organizations. Several participants note that organizations need to develop a sense of responsibility towards their business partners and other organizations on their supply chain and wider business network. It is often mentioned by participants that small firms and micro businesses may not think that they could ever be a target for a cyber attack due to the small scale of their activities, but, nevertheless, they become an easy target by hackers who may use them to reach out to larger organizations down the supply chain:

> *"Responsible cybersecurity is to develop this mindset where cybersecurity is not just the data loss in a specific organization, but rather is kind of that whole sequence of events that may happen and kind of spread the attack and the damage, you know, to a wider group of people." (P8)*

The statement above indicates a mindset of caring for one another in the supply chain and also being aware of cyber risks and their possible impacts across the supply chain. Some participants noted that fostering responsible cybersecurity is done through, for example providing training for third-party partners and ensuring compliance among the supply chain: "*We ensure that our third parties are trained, and we make this training a mandatory requirement.*" *(P6)*

However, challenges exist as there are control issues that make it difficult to enforce compliance on another organization. To overcome these, agreements must be in place that prioritize security, e.g., contracts with anyone in the supply chain must have a security element on them:

> *"I buy a service with the cloud, who is responsible for the security? cloud service or the data owner. In their contract, the cloud service provider will try to shift on the other side of responsibility. So basically, the data owners say, no, the cloud provider is responsible for the data security. Cloud providers, would say, the data should be encrypted. So even if you've got a breach, I owe that owner responsibility to be sure that the data is secure, but you find that in every single part in this workflow they try to shift the responsibility to the next level." (P16)*

Participants emphasized the responsibility of the data owner to ensure their data is secure when transferred to third parties and emphasized that responsibilities should not be transferred. For example, if a bank sends customer data to a credit facility, or a translator, then primarily the bank, as the data owner, must ensure the data is protected during the transfer:

> "*We signed a service agreement with the credit bureau to provide credit scores, the bank shares their database with them for credit scores, at that time the data is not ours it's the credit bureau's, if there a breach happens at the bureau it's their fault, if it happens in transit, it is our fault. When you send the data you cannot transfer the risk if you are the data owner, you are still responsible, you send your data to a third-party and there is a data breach at the third-party, the data owner is still responsible, you cannot transfer the risk." (P16)*

The above statement introduces the notion of stewardship as a way of promoting responsibilities towards others in the supply chain:

"If you think about this in terms of your responsibility to others to the fact that they have let you have their data then you are a steward of that. Being a steward means when people trust us with their information or with their assets or with the future of their organization, that we supply critical services to." (P17)

This statement emphasizes that the data owner is responsible for their data, however, their responsibilities do not end there but extend to data entrusted to a service provider because they are part of a supply chain.

Although small firms in the supply chain face challenges such as limited funding, opportunities to foster responsible cybersecurity exist through external sources such as consultants, cyber resilience groups/initiatives, and AI security:

"We work with quite a few large corporate organizations who help us financially to run the center, but also recognize that kind of cyber security within their supply chains and things like that is really important. And so, we are looking at how we can work with larger companies to reach your supply chain, because if they've got 1000 small businesses that work for them, we can go and help them tap those small businesses because then it will help bigger businesses. But they are part of that supply chain the same way that the smaller companies are, but they've obviously got access to a lot more resources and kind of investment for them, making sure their supply chain is really secure. So, I think a lot of the larger organizations are starting to pick up on some merged responsibilities now." (P6)

Without having to employ their own security teams, small firms can still contribute to the security of their supply chain. Similarly, big firms selling security solutions can also contribute to their supply chains by making their solutions affordable and accessible to SMEs. Yet another

challenge identified involves the rate of churn in the supply chain, necessitating continuous awareness training for newcomers.

Societal-centric Perspective

The societal-centric perspective encompasses a perspective on responsible cybersecurity that goes beyond the organizational (intra- and levels) to considering the wider social and societal impacts of cyberthreats. One participant illustrated one such attack, noting:

> *"When I was in the cyber team, we investigated an attack, ransom attack against a major food supplier and on paper they make food. They made a mass amount of food in the UK. They weren't very mature at the time, so it wiped them out pretty much for a couple of days. To the point if they had gone much further than the point that they did, it would have to go to a national [emergency] meeting to discuss how there's going to be gaps on the food shelves across the UK because the amount of food they were making because the speed at which they make it, it was going through such a rate if they were offline for a week or two, it would leave empty shelves across the UK. So, it's trying to get that understanding. They never thought they were going to be sort of targeted for a cyberattack, but they were. They lost a massive amount of our operational capabilities. That is the kind of impact that it could have." (P6)*

This perspective presents the need to move towards a mindset where the potential ethical and social implications are considered from the onset in the interest of restricting potential harm to the society:

> *"Ethics is about your intention, your purpose and decisions that you make, being intentional about what you create, what you collect so we need to be able to think about, our intention behind, for instance, the collection and the stewardship of information and data and the services that we provide." (P17)*

The challenge linked to this perspective is that concerned parties could indicate a lack of awareness of the potential societal harms associated with what they created. Further, there was emphasis on the practice of ethical by design to ensure security solutions consider ethical implications from the onset:

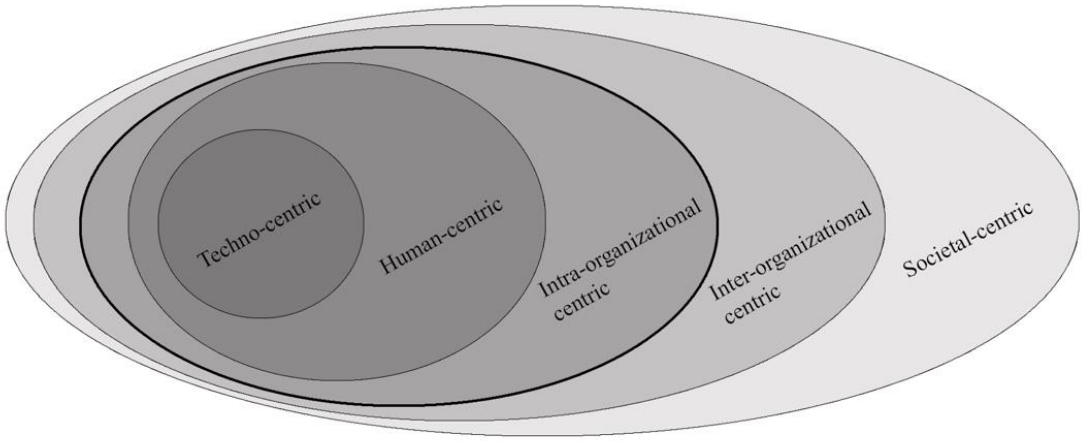
> *"By failing to think about how a service can be misused, it has the potential to lead to untold harms to the rights and freedoms of others …You have got to consider the implications of what you are building. How will it impact diverse communities, so that the whole mentality needs to switch." (P14)*

Further analysis of our results reveals how these perspectives are inter-connected. In the section that follows we show these inter-connections.

Building the Inter-connections: From Different Perspectives to Layers

Though the different perspectives may be seen as initially being distinct and even contrasting (e.g., technology vs human), further analysis has shown that these are in fact best viewed as layers of a wider responsible perspective positioned within an onion-shaped model (Figure 1).

Figure 1: Onion-shaped Responsible Cybersecurity Framework



Each layer represents a critical dimension of an eclectic responsible cybersecurity perspective. However, a layer on its own is not sufficient as this is limited to a group of stakeholders, their specific views on cybersecurity and what this entails. Putting the different layers together assists in forming a holistic responsible cybersecurity framework. Collectively, the layers help to identify the different pillars of responsible cybersecurity and the multiple stakeholders in this domain.

In the inner circle (depicted with darker tones) there are the layers with an internal organization focus. Without underestimating the significance of the human dimension as well as the role of the wider organizational context, in the core of the inner circle, we position the techno-centric layer to show that technology represents the organization's defense against cyber vulnerabilities and attacks.

In the outer circle (depicted with light tones) there are the layers with an external orientation, organizational-centric and societal-centric which represent the organization's responsibility

towards its suppliers and business partners, as well as to the wider society. At the outset of the model, the societal-centric layer is positioned to show the impact of cyber attacks on the wider society

Table 3 shows the inter-connections of the different layers of responsible cybersecurity.

Table 3: Inter-connections of the layers of responsible cybersecurity

	Inner	**Outer**
Responsible Cybersecurity	Techno, Human, and Intra-organizational	Organizational and Society
Significance	*"responsible cyber security challenges and issues are actually a three pronged approach where technology needs to be combined with process and people….you need a union of these three things in the equal to create, in my opinion, what I call responsible cybersecurity, even if you've got one missing piece right? It's not responsible. It's irresponsible." (P1)*	*"they will always be part of a supply chain. They will always be part of some other sort of network, or whether it's their suppliers, their customers and they are response they are in that chain. So if they're hit with a cyber attack, they're potentially going to lose their customers details. They're going to lose other clients details, and that is going to cause some issues with GDPR. It's going to cause issues with their own sort of reputation and that is trying to make that understanding and responsibility for their own cyber security as well as everybody else around them" (P6)* *"one of the biggest threats we encounter is by state actors, I mean countries which want to damage the critical infrastructure in the UK and cause chaos because that's the biggest outcome that anyone can achieve by breaching us." (P8)* *"I think it's not far couple of days before, the three hospitals had a had cyber attack and they had to either cancel their services or had to divert their services to other hospitals. When NHS Lancaster had had disruption due to the cyber attack and I was the part of the team who were who patrolled. We were unplugging the computer from the network so that the malware is not propagating on other systems and I was one of them." (P12)*
Scale	Organization's security	Supply chain security and public security.
Scope	Employees (people), Technology, Processes.	Suppliers, Customers, Venders, third-party, Networks, Ecosystem, Public, Communities.
Best approach to promote	Top-down	Stewardship

responsible cybersecurity		

The relevance of the onion-shaped model in the field of responsible cybersecurity is two-fold: First, it shows the extent and diversity of impact of cyber attacks ranging from technologies to individual-users, entire organizations and their reputation, impacts on the organization's supply chain and on the wider society. Second, the model shows that responsible cybersecurity does not stop at any particular layer but rather it encompasses all layers together ranging from technology-specific to societal centric.

Leaders' Roles in Fostering a Multi-layered Responsible Cybersecurity

Leadership and particularly at senior organizational level, emerged from our analysis as the most influential vector in fostering responsible cybersecurity:

> *"realistically it starts at the top, the CEO, senior leadership stakeholders, are responsible overall and have accountability for security as well. ...a lot of the cyber attacks stem from a lack of understanding at the board level as well." (P5)*

Though frequent reference was made to senior organizational leaders, the role of cybersecurity leaders is indicated as influential:

> *"Getting cybersecurity people talking to senior leaders in a way that they understand what is needed, what the risks are, and what is needed is to create a responsible cybersecurity environment. Because if we, as cybersecurity leaders, can influence and engage with those leaders, those leaders have got the power to be able to then change the culture change. Have a responsible cybersecurity mindset from a top down, it has*

to come from the top-down as opposed to from the bottom-up, because ultimately, it's getting from the top telling everybody what to do at the lower positions. So, it needs to come down in that approach. Because again, it's getting people who understand cybersecurity well enough to then talk in a language and in a way that leaders e.g business leaders can understand." (P10)

Table 4 shows leadership practices at different layers of responsible cybersecurity as these emerged from the data with exemplary quotes. At the techno-centric layer, the ideal practice is for organizational leaders' to finance required technologies: "*the CEO, they are the person responsible for buying the IT" (P18).* At the human layer, having a more people-oriented approach where people are cared for and awareness training is prioritized is considered an effective approach which links in well with building a strong security culture at the organizational layer. Further, leaders play a crucial role in setting the tone at board level discussions, ensuring that cybersecurity is viewed as a core responsibility embedded in the organization's values and culture:

"There needs to be buy-in to the board level. Responsible security can't go bottom-up…
"Organizations must prioritize board-level buy-in for responsible cybersecurity … So that is where you start to have the board is into it, the buy-in and the management budget is assigned to it. So basically, the highest level [of decision] has to be the most important thing and then you start to get budget in how you implement it." (P3)

Leadership provides financial support, enabling the implementation of necessary solutions and programs to safeguard the organization. As role models, leaders exemplify responsible cybersecurity behavior, encouraging others to adopt similar behaviors. By blending these efforts, leadership can successfully cultivate a cybersecurity aware culture, ensuring that all employees contribute to protecting digital assets. They can achieve this by fostering a culture

of awareness and accountability ensuring that cybersecurity is prioritized at all levels. This shift in mindset requires board-level buy-in, where top executives not only understand the importance of cybersecurity but actively commit to its integration into strategic goals.

> *"Responsible cybersecurity starts first with the leadership of the company. The leadership needs to understand the importance and the need of proper cybersecurity. It includes proper support and equipment. Without the understanding and support from the senior management, there is no cybersecurity neither responsible one." (P4)*

Further, participants emphasize reporting security incidents and compliance to regulations in general as a key practice that must be complied with from the highest level of leadership.

Leadership is equally important in fostering a broader cybersecurity awareness in their supply chain. This external influence can help promote a culture of shared responsibility for cybersecurity across the supply chain, encouraging a collective effort to address cyber risks. Moreover, leadership is key at the societal level in promoting ethical awareness of the impact of the actions, statements or products of the organization on the society. As highlighted by our participants, "*things do start at the top*" (P17). When leaders care about and understand the ethical dimension and wider implications of their work, this fosters a culture where employees and stakeholders alike are encouraged to consider the broader impact of their actions. This sense of extended responsibility ensures that cybersecurity efforts are not just focused on protecting the organization, but their impact on society is considered and restricted from the onset. Achieving this requires demands leadership rooted in a core values approach. By demonstrating care, moral courage, and a commitment to ethical practices, leaders ensure that cybersecurity strategies align with societal responsibilities.

Table 4: Leadership practices across the different responsible cybersecurity layers.

Responsible Cybersecurity Layers	Leadership Practices	Exemplary Quotes from Interviews
Techno	Sponsorship and funding	*"..Sponsorship and funding, realistically to show you have the best fight against hackers and bad actors is you need to have the money to invest in the tools that actually protect you." (P17)*
Human	Caring and people-oriented approach	*"Actually this is about managing your workforce so that you don't lose them to burnout. So, there is lots of different types of training out there, but actually if, for instance, at an all-staff meeting, if the CEO said I am going to hand over to the head of people because we would like our staff to set up some employee resource groups, but we don't know what kind of groups to set up because we are not 100% sure of what the company, what you guys or girls want to do and then if, for instance, if the head of people sort of said OK, we have got a budget…" (P13)* *"They have sort of sidestepped the human notion of caring. So when you have commoditized care as something delivered, for example as in the health sector, you may inadvertently forget that caring is something that we do as humans. When I am talking about leadership and mentoring for people, risk, is about responsibilities to ourselves, responsibilities to others and then things like our service level agreements are the mechanisms by which we build those things as a reality…" (P17)*
Intra	Cultural change for shared responsibility	*"Leaders have got the power to be able to then change the culture. Have a responsible cybersecurity mindset from a top down and it has to come from the top down as opposed to from the bottom up, because ultimately, it's getting from the top telling everybody what to do into lower positions." (P10)* *"That requires buying from the top ... If there is no buy in at the top level, it is doomed to failure bottom up." (P3)* *"One that quickly comes into my mind would be. The culture. You know eventually. Where I am right now, I'm actually trying to build. Cyber security aware culture. Hmm. And I believe if. You can start actually doing that and ensuring that management also in that little space they do that that we see all the MD's, they do that as well, ensuring that the highest level customer, the Minister as the Presidents when wherever they have the speech they actually. One line. They have one line that. Speaks to cyber security. Then we will certainly be in in a much a better way. When it comes to having responsible cyber security" (P9)*
	Reporting	*"Security is a program that is taken seriously here, and we ensure that even reporting to the highest level, we do so" (P9)* *"Responsibility lies with the Board of Directors, who are the one who is the legal representative of an organization. So, if you are in charge of an organization, you have to be aware that. If your IT systems fail, you have to. To report what happened." (P15)*

	Risk and Compliance	*"If you are an organization that expects cybersecurity and takes care of it, then you should be compliant. Firstly. the internal people with technical expertise and the appropriate authorization internally, but then they should be transferred to the management of the company because finally these people are responsible board of directors. Or the people in charge of an agency or for public authority." (P17)* *"It needs to be involved at very senior levels to be able to make sure that you know it's not just necessarily a technical risk you're dealing with all parts of the business now feed into a cybersecurity risk." (P11)* *"Cyber leaders define the posture and the risk appetite of the company based on senior management indications of senior management leadership team governance." P17* *"Whether it's the board itself or still, it'll be the senior leader who is at the forefront of ensuring compliance in organizations, ...it's top down." P3*
	Collaborative approach	*"a statement we have had in the past, that there's a disconnect between the security leaders and the business leaders that's actually ending a lot now because security leaders and business leaders actually work together now on objectives." P1*
	Top-down approach	*"Building a security awareness on this level, first on the very senior level on the exec executive level is the most important because without commitment of this level you can't look for anything down." (P4)*
Inter	organizational collaborations	*"If you identify that you have a problem with certain suppliers. Then the discussion to the external partners should be made by the top management. .. the people who are in charge of the organization should be aware (of supply chain risks and problems)." (P17)*
	Supply chain cyber alliance	*"They need to be sponsored so that they can be a part of external communities so that you'd be able to exchange best practices." (P3)*
Societal	Ethical dimension	*"But what we do need is for someone who's in charge, at least to understand the ethical dimension of [cybersecurity practices]." (P17)* *"Things do start at the top and so they the way the system performs in terms of its values and whether people are really thinking about the ethical dimension of their work, for example, that starts with whether the leadership care in that way." (P17)*
		"*then at the top level legislation, passed legislation saying whatever you produce, can't it can't accrue an ethical debt "down the line, you know, shouldn't be any privacy harms to victims. So yeah, make it legislate" (P14)*
	Core values approach	*"... sort of the values approach to leadership. leaders care, leaders have moral courage." (P17)*

Discussion

The driving interests for this study have been to first explore the meaning of responsible cybersecurity, both in terms of scale and scope, and then to identify how to foster a responsible cybersecurity mindset. By adopting a qualitative exploratory approach, we identify different layers of responsible cybersecurity which collectively represent the scope of responsibility in the cybersecurity domain. Following this, we posit that the most effective framework in fostering a responsible cybersecurity perspective is one that takes a holistic approach, ensuring care for securing the technology, while simultaneously ensuring a huge sense of responsibility towards the multiple and diverse stakeholders that might be directly or indirectly affected by potential cybersecurity threats. Our findings point to different perspectives on this theme which we interpret as layers within a proposed framework. With this, we take the position that our onion-shaped framework captures the multi-layered nature of responsible cybersecurity, solidifying our empirical study (Figure 1).

The study shows that responsible cybersecurity consists of multiple layers; the peeling of one layer helps to expose another one. As is the case with onion models, the outer layer is the one that is most visible. Indeed, most of the known cyber attacks are those that have had wider impacts on societies. For example, Advanced, a company providing IT services to the Britain's National Health Service (NHS) was hit by a ransomware in August 2022 (MacColl et al., 2022). The incident resulted in missed GP appointments and house visits. Patients missing crucial operations or chemotherapy sessions, and some in emergency situations not being able to access emergency services emphasizes the wider impact of the cyber attack not only on the company, but also on the general public, through the NHS. More recently (June 2024), Synnovis, a company offering the NHS laboratory services was attacked, resulting in 400GB of patient data stolen, and more than 1,000 operations and 3,000 appointments being missed (Conosco, 2024). These examples indicate the impact of how one single entity in the supply

chain contributes to the disruption of a nation's health system, its critical services, and the wider society. When cyber attacks like these are manifested at societal level, the connections between the different layers, as well as the role of each layer, are gradually uncovered.

In the following section, we discuss the theoretical contributions of the study and in particular how the proposed framework informs existing debates on responsible digital.

First, the study introduces a new theoretical framework on responsible cybersecurity which shows the scope and scale of responsibility that surrounds cybersecurity. Through the inclusion of different and diverse layers that span across techno-centric, human-centric, organizational (intra- and) and societal, it provides an integrative and balanced approach, not only of different views that can be represented in the responsibility domain, but also the multiple and diverse stakeholders who have an interest in cybersecurity and who may be affected by potential attacks. Responsible cybersecurity is realized when all these layers are addressed. Moreover, the framework emphasizes the importance of purposefully considering the need to widening the scope of responsible cybersecurity beyond merely a technological focus, and far beyond organizational-specific boundaries. For example, the societal layer interacts with the technological layer through the development and implementation of technologies that are aligned with societal security. This integration of the different layers creates a holistic and resilient framework where stakeholders collaborate to protect their data, and minimize potential security and privacy harms.

A second contribution of the study is that it expands literature on responsible digital and digital responsibility. Current literature tends to focus responsibility on the design, adoption, and implementation of digital technologies with predominant focus on the role of designers and developers, and how their actions need to be ethical and accountable. Our study shows that a responsible approach for digital initiatives (therein cybersecurity) can be viewed from different

layers, each exposing different stakeholders both internal and external to the organization. The study advances a framework that integrates different and diverse perspectives of responsibility, showing the scale of *responsible* digital by capturing a broad base of individuals within and beyond the organization.

A third contribution is around leadership and governance more broadly. Cybersecurity when managed from a responsible perspective, is not just a matter of cybersecurity professionals. It needs organizational leadership to champion it. The increasing inter-connectivity of systems and networks, along with the prevalence of emerging technologies such as the IoT and AI can potentially amplify the likelihood and impact of security breaches, which span from personal, to organizational, and societal level. Senior organizational leaders need to consider the potential impacts of cybersecurity threats and attacks on society, such as national or international critical infrastructure, and societal well-being overall, and not just within their own organization. This requires a renewed mindset on cybersecurity governance and responsibility. The example of the CrowdStrike breach in July 2024 is illustrative here. The breach revealed the vulnerability of supply chains by affecting over 8.5 million Windows systems world-wide, resulting in the cancellation of services across several sectors, including healthcare, transportation and finance globally (Scroxton, 2024). Considering cyber security from a responsible perspective can, thus, assist in the direction of taming the 'wild problem' of third-party risk management.

Conclusions, Limitations, and Research Implications

This study was driven by an interest to explore responsible cybersecurity to align with the increasing and timely attention being given to responsible digital and digital responsibility. Through a series of interviews, we develop an onion-shaped framework depicting different layers of responsible cybersecurity. Findings point to the important role that leaders have in

developing inter-connections between the different layers. The study makes contributions to the fields of cybersecurity, responsible digital, and leadership.

The study is not without limitations and there are several implications for further research. Given the exploratory nature of the research, interview participants represent different sectors, organizations and positions. As such, sector-level or organization-level views were not included. Thus, further research is needed to carry out an in-depth case study to examine organizational and sectoral mindset towards responsible cybersecurity. In addition, our data collection focuses on people who have direct expertise in cybersecurity, such as CISOS, consultants, and other cybersecurity managers and experts. Future research should also consider the views of other organizational members, such as employees and senior organizational leaders. Doing so will extend a wider and more inclusive view of what responsible cybersecurity is. Moreover, despite our efforts, most of our participants were white and male. Though the sample is representative of the demographics of the cybersecurity profession, the study did not include a balanced and representative view of minority groups. Future research in this area should address this. Moreover, further research that examines small firms and their reliance on external cyber support is also encouraged with a focus on the role they play in organizational centric responsible cybersecurity.

The onion-shaped framework of responsible cybersecurity establishes the foundations for future research and prompts for more systematic thinking around responsible cybersecurity. In particular, it contributes to the expansion of the research agenda on responsible digital and responsible cybersecurity. It prompts for an examination of the different roles that can be enacted at different layers, and how these layers are linked. Our study identifies leaders as a key vector in this process, but further research is needed to explain what this entails. One particular area is related to the aforementioned vulnerabilities of global supply chains. These

indicate the need for further research on the role of leaders in ensuring effective global organizational collaborations from a responsible cybersecurity perspective. Research is also needed to expose the inter-connections between the different layers of the framework. Though the study provides evidence on the links between specific layers, there is a need for a deeper understanding of how different layers interact with and impact each other.

Implications for Practice

The study provides several implications for practice. First, the proposed onion-shaped framework can serve as a tool which cultivates and supports a positive security culture within organizations, since shared responsibility is one of the components which promote active involvement with cybersecurity. The promotion of such a security culture is of direct benefit to all roles within an organization, from employees, to managers, to senior leadership as it affects the norms, interactions, and the nature of support within the organization. The effects of responsibility, however, are broader, pervading security attitudes, behaviors, and communications within a given environment. These, in turn, can assist in training and educating individuals and shape norms which can foster security hygiene, i.e., can be reducing the attack surface by shaping appropriate practices. All these underlying components are eventually manifested as individuals' compliance-related conduct. However, compliance can be regarded as a beneficial byproduct of these driving forces rather than the ultimate objective, as individuals have the potential to shape their overall security perceptions and behaviors by adopting a responsible cybersecurity ethos. Nevertheless, the goals of safeguarding against regulatory fines and reputational damage, set by *compliance officers,* are directly supported. Second, the framework can be utilized as a tool for various security roles such as CISOs and other cybersecurity professionals. Within organizations, the need, requirements, and implementation of security mechanisms can be analyzed across the different framework layers.

At a high level, *policy makers* can consider policies, procedures, and guidelines to harmoniously span across the framework layers. The binding of the technical component with the human and intra-organizational ones is critical beyond traditional security awareness training and education, for understandability, usability, acceptability, and efficiency. The importance of this binding expands equally to more technical security roles such as *security operations* professionals, *security architects*, and *incident response teams.* In particular, the alignment of security architectures with business and industry objectives, the monitoring of attacks and threats, data protection approaches, forensics investigations, incident response plans, and incident reporting, are all components which can benefit from the layered structure of our proposed framework. For implementations, the analysis can take place both *prior* to their deployment, i.e., as a means to identify requirements, and *after*, i.e., as a means to evaluate their effectiveness across the layers. Along with security controls, security professionals can introduce interventions to change the security behavior of individuals within organizational environments. *Decision makers* can identify issues related to peer organizations, entities in the supply chain, and the broader security ecosystem, and prioritize security investment collaboratively with *risk analysts* and *cyber threat intelligence analysts* in light of a broader risk exposure view. The role of *CISOs*, as responsible for the overall security strategy, is assisted via the aforementioned areas of policy-making, risk communication, education and training, compliance, and incident response, overall. Importantly, the scope of responsible cybersecurity can provide a lens to consider, create, and evaluate broader, society-wide cybersecurity behavior change campaigns by governments, standardization organizations, and industry bodies, including public-private sector partnerships and national cybersecurity coordination.

Declarations

Ethics approval and consent to participate

Ethical Approval and Consent to Participate was granted by Lancaster University, March 2024. (LU 2024-4329-RECR-3).

Consent for publication

Participants gave their consent to use their data for publication purposes by signing the Consent to Participate form.

Availability of data and material

Study data can be provided upon request by the first author.

Competing interests

None

Funding

This research was supported by funding from *Security Lancaster, Lancaster University* under grant number IRL 1042. We would like to express our gratitude for their financial support, which made this work possible. The views expressed in this paper are those of the authors and do not necessarily reflect the views of the funding organization.

Acknowledgements

We are grateful to all participants of our study who willingly gave up their time to take part in the study and share their experiences. The study would not have been possible without their participation.

Authors' contributions

Professor Panteli contributed to the study conception and design, developed the theoretical foundations and theoretical contributions of the study. Data collection and analysis were performed by Dr Nthubu and Professor Panteli. The Findings section was written by Dr Nthubu. Dr Mersinas contributed by reviewing literature on cybersecurity and developing the practical implications of the study. All authors contributed significantly to the initial drafts and subsequent revisions, with each author focusing on distinct aspects of the paper. All authors have read and approved the final version of the manuscript.

References

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), 1-15.

Bacq, S., & Aguilera, R. V. (2022). Stakeholder governance for responsible innovation: A theory of value creation, appropriation, and distribution. *Journal of management studies*, *59*(1), 29-60.

Barello, S., Triberti, S., Graffigna, G., Libreri, C., Serino, S., Hibbard, J., & Riva, G. (2016). eHealth for patient engagement: A systematic review. *Frontiers in Psychology*, *6*(January), 1–13. https://doi.org/10.3389/fpsyg.2015.02013.

Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). Exploring age and gender differences in ICT cybersecurity behavior. *Human Behavior and Emerging Technologies*, *2022*(1), 2693080

Carpenter, P., & Roer, K. (2022). *The Security Culture Playbook: An Executive Guide To Reducing Risk and Developing Your Human Defense Layer*. John Wiley & Sons.

Carroll AB (1991) The pyramid of corporate social responsibility: toward the moral management of organizational stakeholders. *Bus Horizons* 34:39–48

Choo, K. K. R., Puthal, D., Liu, C. Z., & Wang, C. (2022). Introducing the Special Topic on "Mitigating Cyber Threats and Defense in Data Intensive Smart Cities". *Information Systems Frontiers* **24(5)**, 1393–1394. https://doi.org/10.1007/s10796-022-10354-6

Conosco (2024) NHS Cyber Attacks June 2024. Available at https://conosco.com/in-the-news/nhs-cyber-attacks-june-2024. [Accessed 26 September 2024].

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational research methods*, 16(1), 15-31.

Gioia, D. (2021). A systematic methodology for doing qualitative research. *The Journal of Applied Behavioral Science*, 57(1), 20-29.

Dignum, V. (2019). Responsible Artificial Intelligence*: How to Develop and Use AI in a Responsible Way*. Springer International Publishing. https://doi.org/10.1007/978-3-030-30371-6.

Dimitrov, W. (2020). The impact of the advanced technologies over the cyber attacks surface. In *Artificial Intelligence and Bioinspired Computational Methods: Proceedings of the 9th*

Computer Science On-line Conference 2020, Vol. 2 9 (pp. 509-518). Springer International Publishing.

Duncan, R. (2020). What does 'secure by design' actually mean? *Network Security*, 2020(10), 18-19.

Durnell, E., Okabe-Miyamoto, K., Howell, R. T., & Zizi, M. (2020). Online privacy breaches, offline consequences: Construction and validation of the concerns with the protection of informational privacy scale. *International Journal of Human–Computer Interaction*, *36*(19), 1834-1848.

Kumar, P., Dwivedi, Y. K., & Anand, A. (2023) Responsible artificial intelligence (AI) for value formation and market performance in healthcare: The mediating role of patient's cognitive engagement. *Information Systems Frontiers*, *25*(6), 2197-2220.

MacColl, J., Hüsch, P., & Nurse, J. R. C. (2022) Beyond the Bottom Line: The Societal Impact of Ransomware. Available at https://www.rusi.org/explore-our-research/publications/commentary/beyond-bottom-line-societal-impact-ransomware. [Accessed 28 September 2024].

MacQueen, K. M., McLellan, E., Kay, K., & Milstein, B. (1998). Codebook development for team-based qualitative analysis. *Cam Journal*, *10*(2), 31-36.

Merhi, M.I. (2023)An Assessment of the Barriers Impacting Responsible Artificial Intelligence. *Information Systems Frontiers* **25**, 1147–1160 (2023). https://doi.org/10.1007/s10796-022-10276-3

Mikalef, P., Conboy, K., Lundström, J. E., & Popovič, A. (2022). Thinking responsibly about responsible AI and 'the dark side'of AI. *European Journal of Information Systems*, *31*(3), 257-268. DOI: 10.1080/0960085X.2022.2026621

Mortelmans, D. (2019). Analyzing qualitative data using NVivo. *The Palgrave handbook of methods for media policy research*, 435-450.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization*, *17*(1), 2-26.

Mihale-Wilson, C., Hinz, O., van der Aalst, W., & Weinhardt, C. (2022). Corporate digital responsibility: Relevance and opportunities for business and information systems engineering. *Business & Information Systems Engineering*, *64*(2), 127-132. https://doi.org/10.1007/s12599-022-00746-y

Owen, R., Macnaghten, P., Stilgoe, J., (2012) Responsible research and innovation: From science in society to science for society, with society. *Sci. Public Policy* 39, 751–760.

Owen, R., Pansera, M., (2019) Responsible Innovation and Responsible Research and Innovation, in: Handbook on Science and Public Policy. Edward Elgar Publishing.

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), 103-128.

Pappas, I. O., Mikalef, P., Dwivedi, Y. K., Jaccheri, L., & Krogstie, J. (2023). Responsible Digital Transformation for a Sustainable Society. *Information Systems Frontiers*, 1-9.

Reddy, E., Cakici, B., & Ballestero, A. (2019). Beyond mystery: Putting algorithmic accountability in context. *Big Data & Society*, *6*(1), 2053951719826856.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442-451.

Safa, N. S., Von Solms, R., & Futcher, L. (2016). Human aspects of information security in organizations. *Computer Fraud & Security*, *2016*(2), 15-18.

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., ... & Jinks, C. (2018). Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & quantity*, *52*, 1893-1907.

Sewak, M., Sahay, S.K. & Rathore, H. (2023). Deep Reinforcement Learning in the Advanced Cybersecurity Threat Detection and Protection. *Information Systems Frontiers* **25**, 589–611. https://doi.org/10.1007/s10796-022-10333-x

Scherer, A. G. & Palazzo, G. (2011). The new political role of business in a globalized world: A review of a new perspective on CSR and its implications for the firm, governance, and democracy. *Journal of Management Studies*, 48, 899–931

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. W.W. Norton & Company.

Schultze, U., & Avital, M. (2011). Designing interviews to generate rich data for information systems research. *Information and organization*, *21*(1), 1-16.

Scroxton, A. (2024), CrowdStrike update chaos explained: What you need to know | Computer Weekly

Trocin, C., Mikalef, P., Papamitsiou, Z. *et al.* (2023). Responsible AI for Digital Health: a Synthesis and a Research Agenda. *Inf Syst Front* **25**, 2139–2157. https://doi.org/10.1007/s10796-021-10146-4

Vassilakopoulou, P., Parmiggiani, E., Shollo, A. & Grisot, M. (2022). Responsible AI: Concepts, critical perspectives and an Information Systems research agenda . Scandinavian Journal of Information Systems, 34(2), 89-112. https://aisel.aisnet.org/sjis/vol34/iss2/3

Voegtlin, C., Scherer, A. G., Stahl, G. K., & Hawn, O. (2022). Grand Societal Challenges and Responsible Innovation. Journal of Management Studies, 59(1), 1-28. https://doi.org/10.1111/joms.12785

von Schomberg, R. and Hankins, J. (2019). *International Handbook on Responsible Innovation: A Global Resource*. Cheltenham: Edward Elgar Publishing.

Wang, Y., Xiong, M., & Olya, H. (2020). Toward an understanding of responsible artificial intelligence practices. *53rd Hawaii Internationational Conference on System Sciences*. Maui, Hawaii, USA.

Wheatley, S., Maillart, T., & Sornette, D. (2016). The extreme risk of personal data breaches and the erosion of privacy. *The European Physical Journal B*, *89*, 1-12.

World Economic Forum. (2022). The shortfall of women in cybersecurity is due to lack of support, not access. *World Economic Forum*. Available at https://www.weforum.org/agenda/2022/09/cybersecurity-women-stem/. [Accessed 10 Sep 2024].

Young, J. C., Rose, D. C., Mumby, H. S., Benitez-Capistros, F., Derrick, C. J., Finch, T., & Mukherjee, N. (2018) A methodological guide to using and reporting on interviews in conservation science research. *Methods in Ecology and Evolution*, *9*(1), 10-19. https://doi.org/10.1111/2041-210X.12828.

Zamani, E., Angelopoulos, S. & Conboy K. (2023). Special Issue: Being Responsibly Digital, *Information Systems Frontiers*.

Zhang, J., & Hon, H. W. (2020). Towards responsible digital transformation. *California Management Review Insights*.