“Where Are We On Cyber?” – A Qualitative Study On Boards’ Cybersecurity Risk Decision Making

Jens Christian Opdenbusch*, Jonas Hielscher*, M. Angela Sasse*†
*Ruhr University Bochum, Germany † University College London, UK

***Abstract*—Boards are increasingly required to oversee the cybersecurity risks of their organizations. To make informed decisions, board members have to rely on the information given to them, which could come from their Chief Information Security Officers (CISOs), the reports of executives, audits, and regulations. However, little is known about how boards decide after receiving such information and how their relationship with other stakeholders shapes those decisions. Here, we present the results of an in-depth interview study with $n = 18$ C-level managers, board members, CISOs, and C-level consultants of some of the largest UK-based companies. Our findings suggest that a power imbalance exists: board members will often not ask the right questions to executives and CISOs since they fear being exposed as IT novices. This ultimately makes boards highly dependent on those providing them with cybersecurity information, leading to losing their oversight function. Furthermore, cybersecurity risk is abstracted to budget decisions with no further involvement in cybersecurity strategies through boards. We discuss possible ways to strengthen boards' oversight functions, such as releasing industry benchmarks through public cyber agencies or implementing support structures within the company - such as standing (cybersecurity) risk and audit committees.**

I. Introduction

Most organizations today rely on digital assets and infrastructure. But the technology organizations rely on is vulnerable. Attackers have found many ways of attacking organizations: whether it is intellectual property theft – which FBI Director Christopher Wray called the largest wealth transfer in history[1] – social engineering to trick employees into transferring large sums of money to the wrong accounts, or extorting money via ransomware [1]. For many years, security experts have demanded that organizational leaders – and specifically boards – pay more attention to digital risks [2], [3], [4], and invest more to reduce vulnerabilities or make it harder to exploit them. However, since the number of incidents and losses keeps increasing [5], [6], many organizations are still not doing enough or doing it wrong.

In the Western hemisphere, governmental and non-governmental agencies have created laws and regulations to encourage organizational leaders to ensure at least a basic level of protection, which has given rise to a whole industry of auditing and certification around cybersecurity. While these external drivers and actors can improve protection, there are indications that company leaders remain largely detached from cybersecurity decision-making, e. g., when Chief Information Security Officers (CISOs) report numbers to the board that they know have no value but are nevertheless demanded by the board [2]: “If I go to the leadership and say we need time, then I don’t get it, if I show the phishing simulation numbers, then it works.”.

National technical authorities for cybersecurity, like the National Cyber Security Centre (NCSC) in the United Kingdom, explain to company leaders that “cybersecurity is so much more than a compliance function or the implementation of technical controls” [7]. This raises the question of why leadership in many organizations still does not seem to understand and/or manage the risks of the digital assets and infrastructure they rely on (the *cybersecurity risk*) well enough.

At the top of any stock-traded company, the board of directors – which is composed of executives and non-executive directors (NEDs) in the UK – are tasked with overseeing all risks of the company [8], including cybersecurity risks [9], [10], [11]. To fulfill their tasks, they typically rely on reports, e. g., from the Chief Financial Officer (CFO), who will report any credit default. They then have to make strategic decisions based on those reports. Regarding the relatively new form of cybersecurity risks, it is unclear who presents the information, what information is provided, what boards make of it, and what decisions they can make. Some previous research with CISOs hints at boards treating cybersecurity risks differently than other existential risks: “[CISOs] perceive a lack of awareness for security among the board members.” [2].

While a wide range of white papers with instructions for boards from regulators and consultants are available, almost no studies with board members exist. More particularly, no one explicitly studied how boards perceive and handle cybersecurity risk within the largest companies – one reason being that top-level leaders of large companies are notoriously hard to recruit for researchers. Consequently, it is not understood whether cybersecurity risk is handled as outsiders would expect and whether it is dealt with appropriately.

[1] https://www.forbes.com/sites/russellflannery/2020/07/07/china-theft-of-us-information-ip-one-of-largest-wealth-transfers-in-history-fbi-chief/, accessed February 4, 2025

Network and Distributed System Security (NDSS) Symposium 2025
24-28 February 2025, San Diego, CA, USA
ISBN 979-8-9894372-8-3
https://dx.doi.org/10.14722/ndss.2025.240595
www.ndss-symposium.org

We therefore formulate the following research questions

Q1: **How does cybersecurity risk decision-making of boards work?** *We want to understand the information flow toward the board, the type and content of their decisions, and how they are executed.*

Q2: **How do other stakeholders influence those decisions?** *We want to understand how CISOs, executives, regulators, investors, and others influence cybersecurity risk decision-making.*

Method: We performed a qualitative, in-depth interview study with $n = 18$ UK-based top-level leaders (6 executives, 4 NEDs, 5 CISOs, 3 C-level consultants) from some of the largest organizations, with tens to hundreds of thousands of employees and multi-billion pounds in turnovers. Through the interviews, we got deep insights from different angles – with 9 participants sitting on boards and 8 working with and reporting to boards. We asked questions about the historical development of cybersecurity risk at boards, the concrete structures to handle cybersecurity risks, their challenges, expertise, perceptions, and how stakeholder relationships shape the board's work.

Findings: We find that CISOs and executives aim to talk the language of risk with the board, equivalent to other business risks. But without NEDs understanding such cybersecurity risks and CISOs struggling to translate cybersecurity risks into more general risk comparisons to other business risks, no common ground for conversations on eye level can be established – which would be crucial for an informed security strategy. While boards need to have oversight about all risks and are ultimately responsible for failed risk controls, their decisions are, in most cases, exclusively built around budget decisions and investments: NEDs are satisfied as long as executives and CISOs tell them that they invest enough. Boards lack measurements to verify whether the cybersecurity risk is accounted for appropriately beyond general audits and subsequent reports.

Contributions: (I) To the best of our knowledge, we are the first to study the in-depth perspective on cybersecurity risk from top-level leaders from some of Europe's largest companies. (II) We explore how the concept of *risk* is used as a way to communicate about cybersecurity at the highest levels, but also why this *language of risk* has limits in establishing a common ground for communication between boards and CISOs. (III) We show that the CISOs are the ones in power – due to some NEDs being afraid to get exposed when asking technical questions –, leading to a loss of the oversight function of boards. (IV) We show that even though the concept of risk management is well embedded in such large organizations, the transfer of already existing risk management concepts to cybersecurity risks is lacking.

II. Background & Related Work

Here we provide background information (Section II-A) and related work (Section II-C) about boards of directors and how they (should) manage cybersecurity risks (Section II-B), as well as the role of CISOs within organizations (Section II-D).

A. Boards

Large companies' management – especially stock companies – is organized differently worldwide, even within the economically harmonized Western world. It is common to split day-to-day business and the oversight between bodies. In the UK, where we conducted our study, the board of directors has an oversight role. It typically consists of some of the company's executives (like the CEO, CFO, or Chief Information Officer - CIO) and additional non-executives (NEDs). While the executives work full-time on the daily operations, the NEDs will come together to board sessions a few times annually to perform their oversight role. In contrast to this, e. g., in Germany and Austria, the board of directors solely consists of NEDs. Georg et al. [12] noted that it is pretty important to explicitly distinguish those board models when one performs cybersecurity research. When we speak of *boards* in this paper, we always refer to the **board of directors**, and sometimes we directly make statements about NEDs, excluding executives that are also part of the board.

B. Boards & Risk

Managing corporate risks is a governance issue that is "squarely within the oversight responsibility of the board" [13]. Opitz [14] is thus calling for making cybersecurity "a topic on the agenda of each board meeting" and also "treating cybersecurity like any other business risk." The majority of NEDs in the US believe that cybersecurity risk is the most challenging risk they have to oversee [11]. The existing and monitored non-cybersecurity risks often pass through a *Risk and Audit Committee* before reaching the board. According to Lankton et al. [15], cybersecurity is currently underrepresented and poorly understood at such committees. Heroux et al. [16] found that boards can best work with cybersecurity risks when installing a specific subcommittee to those tasks. Higgs et al. [17] found similar for *technology committees*, while others found that companies often lack those [18], [19]. In theory, boards should set the right *risk appetite* [20] for their organizations: an abstract concept that describes how investment should be balanced with risks. The *directors' handbook on cyber-risk oversight* is a regularly updated body of knowledge that should guide boards in this manner [21]. The first chapter acknowledges CISOs as an important entity within a company that has to manage "vast numbers of operational, reputational, and monetary risks." Further, this handbook gives examples of what boards should ask a CISO. While some of these questions circle investments and budgeting, they also suggest more interactive engagements outside the boardroom, such as accompanying the CISO. At the same time, they assess threats or conduct "exercises to test the effectiveness of cybersecurity controls."

Previous studies suggest that boards still lack IT expertise [22], [23]. In 2017, Bonime-Blanc [24] laid out how a successful cybersecurity risk strategy for boards could work and especially stressed that board members would "need to ask the right questions" and again that subcommittees for cybersecurity would be key. Vincent et al. suggested the same [25].

C. Security Research With Top-Level Leaders

Most research on the board members' relationships with cybersecurity is based on publicly available company information [26], [27] rather than on direct (interview & survey) studies with and about the subjects. We do not consider the studies by consulting companies who regularly claim to study boards' perspectives on cybersecurity [28] as sound research in this context. While consultants bring additional perspectives and expertise, they also have their business interests, and the methodologies and data from which their recommendations are derived are undisclosed in their publications. Gale et al. [29] conducted one of the few academic interview studies. They interviewed 18 participants (solely consisting of NEDs) on their perception of cybersecurity duties. The researchers concluded that NEDs showed insufficient commitment to cybersecurity. In 2007, McFadzean et al. [30] interviewed 43 executives and found that their engagement with cybersecurity risk varied heavily between organizations. Wallace et al. [31] interviewed a small sample of 7 C-level executives and IT consultants to understand concerns and influences of adoption decisions for cybersecurity. They evaluated the Technology Organization Environment (TOE) Framework and concluded that it was "useful but insufficient for examining cybersecurity adoption decisions" and should be extended. Abraham et al. [32] interviewed 45 leaders from US-based healthcare organizations, including board members and executives, on how they managed cybersecurity risk. They concluded that boards were aware that they were currently just *muddling through*, were longing for cost estimates associated with cybersecurity risks, and that some executives aimed to train NEDs on cybersecurity specifically. A non-representative survey with 200 board directors [33], found that directors expected CEOs to handle cyber security and not a CISO, as their role description would suggest. Through reviewing publicly available data of board decisions from over 2,000 companies, Klein et al. [27] found that the introduction of the GDPR – as a major EU-located cybersecurity risk-related regulation – attracted attention to cybersecurity risk topics and got them onto board agendas. Reviewing companies' annual financial reports, Smaili et al. [26] found that "Independent members of the board, acting as a governance and oversight mechanism, significantly increased the disclosure of cybersecurity risks in the company's financial statements". Investigating public data from 208 tabletop game sessions (44 of which included board members), Shreeve et al. [34] did not find significant differences in decision-making performance by comparing players' backgrounds and team diversity. In contrast, Radu et al. [35] studied board decisions of 60 companies to disclose cybersecurity risk reports and breaches and found that those with more female members disclosed more. The same was found by Mazumder et al. [36].

D. CISOs

Chief Information Security Officer (CISO) is a diverse term for the head of cybersecurity at an organization. Still, depending on the organization's size, this can mean anything from a lone wolf in the IT department to an executive team member with hundreds of professionals reporting to them [37], [38], [32]. In our participants' organizations, all CISOs lead larger teams and directly report to the board or an executive. CISOs often face difficulties in gaining credibility within their organization due to, among other things, their unclear role, identity, and their perceived lack of power [3]. The role of CISOs shifted from being technical, IT-heavy [39], [40], [41], [42], to more of a leadership and governance oversight role [39], [40], [41], [42], [43], [44], [45], [46], [47]. A significant number of researchers tried to identify how CISOs should position themselves in their organizations, how they (should) collaborate with employees and management and what challenges CISOs still face when they try to integrate them into normal business processes [2], [41], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60]. The majority of research concludes that CISOs sit between the chairs and have trouble to be understood by other stakeholders.

III. Methodology

We aimed to understand how boards (executives and NEDs) perceive cybersecurity risk issues and their experience in managing them. We performed interviews with $n = 18$ participants holding either top-level positions (executives, NEDs, C-level consultants) or leading cybersecurity (the CISOs) in large UK-based enterprises, meaning they all had decades of experience. Five researchers (R1-R5) were involved in the study that took place in the first six months of 2021. The delay in submitting the results for publication is due to labor-intensive transcription and redaction, plus multiple stages of reviews by participants' organizations. Figure 1 summarizes our methodology.

A. Instrument Development

The interview guide was developed by three researchers (R3-R5) in multiple stages. The starting point for the project was a concern by cybersecurity professionals – including those in relevant UK government agencies – that *boards were not doing enough* to understand and manage the cybersecurity risks their organizations faced. Therefore, we started with questions exploring interviewees' perceptions of cybersecurity risks the organization faced and how it handled them. We explored those with two key members of the Advisory Board to our research project (a former CIO in a large global enterprise who had held multiple NED appointments and was regarded as particularly *cyber-savvy* in corporate and government circles and an active CISO of a global technology company with 20+ years experience). They put us in touch with six experienced participants who were willing to be interviewed informally (not recorded) to help with problem exploration and scoping; from their input emerged (I) different models of board decision-making, (II) different lines of reporting, roles, and structures, and (III) how information on cybersecurity presented to the board is collected and prepared. R3 conducted these interviews (with a CISO, a NED, two senior risk managers, the leader of a body of auditors, and a leading government expert on cybercrime) and took detailed notes. Topics covered all aspects of NEDs' and executives' roles in security decisions and their relation to CISOs. Those notes were shared with the research team and guided the development of the interview guides through three sessions of reviews and discussions. See Appendix A for the complete interview guides. The interviews covered the topics of (I) board structure and relationship, (II) security decision-making, and (III) security metrics and communication.

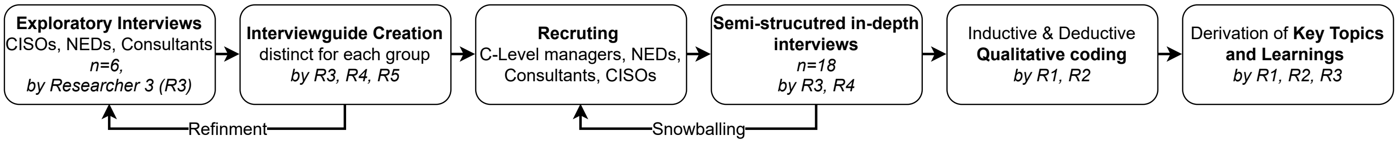

Fig. 1. Our methodology.

B. Recruitment

NEDs and executives of large organizations are notoriously busy, so getting them to find time for interviews is a challenge; additionally, there is always a concern that discussing security in their organization might reveal sensitive information. We obtained our initial contacts through NEDs and CISOs serving on the Advisory Board of a research program co-funded by the UK technical agency for cyber security (NCSC), created to foster research collaboration between academic security researchers and the industry. The Advisory Board members introduced us to current colleagues, former colleagues, and collaborators. Their standing in the community and the association with the co-founder created an understanding that the researchers could be *trusted* to conduct the interviews and use the information they revealed responsibly. Since the research focused on boards and board members, our participants all work with large organizations (tens or hundreds of thousands of employees and turnovers in billion pounds). The initial interviewees drew on their network of contacts and introduced us to further board members or CISOs who dealt directly with boards, which they considered to have significant experience and good insight into how cybersecurity risk was handled at the highest level (snowballing). This process of building rapport and gaining access to this population took us around 7 months. Due to the ongoing COVID pandemic, our participants were engaged in crisis management in their organizations, and about 1/3 of the proposed contacts did not respond or declined.

C. Conducting the Interviews

The interviews were conducted via an online conference tool approved by the IRB and the Data Protection Officer of the research organization. The interview guide was shared with participants in advance. R3 conducted the interviews and asked the majority of questions, trying to cover all areas of the interview guide while letting the interviewees determine the order in which areas were tackled. R4 dealt with the technical side of the conference tool and recording and asked questions towards the end of the interview that had been missed. A professional high-end transcription service, a vetted and approved vendor of the research organization, transcribed the interviews. We followed an already established protocol for transferring audio recordings and transcripts between the researchers and vendors. We also provided additional instructions for redacting identifying information: replacing organization names with an industry sector label and any individual names with role labels. R4 checked and further redacted potentially identifying or otherwise sensitive information, and R3 conducted a further check before passing the redacted transcripts to the interviewees themselves or their support staff for checking (only three further redactions were requested).

D. Data Analysis

We applied Kuckartz's [61] process scheme of content-structuring analysis – based on Braun & Clarke's [62], [63] theory of thematic analysis, where we used the 'codebook style' coding –, combining deductive and inductive coding strategies and a category-based evaluation along main codes. The coding was done with MaxQDA and happened in multiple steps. It was carried out by R1 and R2 – both experienced coders. With this, we increased the independence and objectivity of the coding since R1 and R2 were neither involved in the instrument development nor the interviews. R3 participated in the final step of deriving key learnings from the finished coding in the final discussions. We reached saturation after coding the first 15 interviews. The coding happened in multiple steps:

(I) R1 and R2 created distinctive deductive codebooks based on the interview guide.

(II) R1 and R2 independently coded the same three interviews: deductive and inductive.

(III) The resulting codebooks were merged.

(IV) This was followed by joint coding of three further interviews and codebook refinement.

(V) R1 coded all remaining 15 interviews.

(VI) This was followed by R1 proofreading and reworking all 18 interview codings.

(VII) In a final step, R1 and R2 reviewed all 18 interviews in multiple rounds of discussion until full agreement was reached. Along with the discussions, multiple memos were created that guided identifying patterns.

(VIII) R3 reviewed the coding and selected quotes to avoid misinterpretation.

E. Ethics & Data Privacy

Our institutional review board approved the study. We followed the principles of the Menlo Report of security research [64] and identified the de-identification of the participants as a significant risk we needed to address. All participants received a consent form that informed them about their rights (following the strict European GDPR that still fully applied to the UK in 2021) and the approved third-party transcription service. They were asked again to consent to be interviewed and recorded at the beginning of the interviews (and all 18 did). While recording the interviews, some participants stated that *they would like to say something off the record*. We removed those statements from the transcripts. Due to the potentially sensitive information involved, we allowed the participants to review the transcripts and ask for statements to be amended or removed. While no participant did, the final approval process delayed the start of our analysis significantly. The audio files were deleted after transcription, and the transcripts were anonymized. To prevent re-identification, we report only limited demographic data. We did not compensate the participants but instead offered to share our results and recommendations prior to publication.

F. Limitations

Our study has a number of limitations: we studied the perspective of a limited number of top-level leaders from large organizations only. Those leaders might perceive the topic of security differently than leaders of small- and medium-sized enterprises – as previous studies indicate [65], [66]. Through our initial recruitment channel, the NCSC, we might have a biased participant sample of NEDs and executives who dedicate more thoughts on cybersecurity risks. However, through snowballing, we also recruited participants unrelated to the NCSC. We conducted our study in the UK. Here, boards work differently than e. g., in Germany, where executives could not be a member of the board. Hence, the same study method might reveal different key topics in other companies and business cultures. Our sample of $n = 18$ participants gave us deep insights into boardroom cybersecurity risk decision-making. They can, however, not be used for generalization.

IV. Results

Here, we present our results, derived from the qualitative coding and the subsequent analysis and discussions.

A. Demographics

All our participants worked in the UK. We interviewed six C-level executives (abbreviated as *EX*), four NEDs, five CISOs, and three consultants (abbreviated as *CON*). Some of our participating NEDs previously worked as executives, and some executives currently work as NEDs. When we refer to a NED or executive, we refer to their current primary role. Some statements of the participants nevertheless reflect their experiences from different roles. Since boards in the UK consist of both NEDs and executives, we interviewed 9 board members – one executive did not attend their company's board meetings. To preserve the anonymity of our participants, we only report key demographic data in an aggregated form in Table I.

B. Cybersecurity Risk at the Board Room

All participants stated that cybersecurity risk was increasingly brought up on board agendas, and no one was aware of an organization where the board would not talk about it, no matter how little the board members liked this topic. Based on the experience of our participants, it was uncommon for boards to make *direct decisions* regarding cybersecurity, e. g., *"The board does not really make decisions. They look at what we do and ask questions, but in the last two/three years I have been here we never did something that was dictated by the board."* – [CISO1]. Most participants (NED1,3,4; EX1,3-6; CISO1-3) explained that simply *setting the right level of budget* for cybersecurity would be the only (abstracted) decision boards are involved in: *"They want to know that I have got enough investment, which they always ask me around, 'Are we giving you enough money?'."* – [CISO3]. CISO2 extends on the guessing game of budgeting by reporting that they had to ask for less budget: *"I had to explain, ' I need less money. I need more of that [challenging] instead.'"* – [CISO2].

TABLE I. Background information of the participants.

Gender		#	%
Male		16	*89%*
Female		2	*11%*
Job Title			
Executive		6	*33%*
Non-Executive (NED)		4	*22%*
CISO		5	*28%*
Consultant		3	*17%*
Industry			
Banking		5	*28%*
Telecommunication		4	*22%*
Logistics		3	*17%*
Consulting		3	*17%*
Energy		1	*6%*
Technology		1	*6%*
Public sector		1	*6%*
Number of Employees			
Max	260,000	*Average*	88,900
Min	5,000	*Median*	94,000
Interview Duration [min]			
Max	62	*Average*	48
Min	37	*Median*	49

1) Asking the Right Questions: Beyond investment decisions, all participants saw the primary *task* of NEDs as *asking the right questions* towards the executives, the CISO, or the security team: *"So, for me clearly the actual management of securing the company and ensuring that there is a right cybersecurity policy and everything else that goes around it, is clearly the management's responsibility, it's not the boards. [...] it's very important that the board is able to ask the right kind of questions about ensuring that the management has the rigor in place as far as the cybersecurity is concerned."* – [EX6]. Regarding what would be the right questions, the majority of participants preferred questions around risk and appropriate mitigation, e. g., *"I think it is more about probing on, (a) what the risks are, (b) how vulnerable the company is to losing access to its IT, (c) what mitigations it has in response, how often it practices, how it trains and how it recovers."* – [NED2]. One of the few exceptions was EX6, who wanted to hear technical questions from the board: *"I've seen a lot of boards the best question that you will get and I don't mean to be offensive is 'Have you had penetration testing?' So that's the best question that you can get. Very rarely will you get any question beyond that"* – [EX6]. Preparing for crisis and exercising emergency procedures was seen as the second big task for boards (see Section IV-B2). Only EX6 and CISO4 wished for boards to have classical leadership roles, mainly to enforce cybersecurity policies in the organization and support the CISO's efforts directly.

2) NEDs Shouldn't Manage Crises: Boards primarily consist of (former) executives. This can lead to the board wanting to get involved in daily operational issues, which the executives might more efficiently solve without board involvement: *"Sometimes the executive committee and the CEO would prefer the main board did not get too much involved in daily* *operational issues"* – [CISO5]. Even more difficult would be the tendency of board members to get involved in crises as NED4 explained: *"Quite wrongly when there is a disaster or something has happened, they [the board members] do like to get involved and take command and they're the wrong people to do that of course. They should be kept informed but they shouldn't be flying the plane."* – [NED4]. During such crises, the board should focus on supporting the executives in handling it: *"The board's role is to create time and space for the executive to concentrate on the problem."* – [EX3]. EX3 even extends on the importance of the board backing their executives by giving the following example before comparing it to the data breach of TalkTalk in 2015 [2] – an incident NED1, 4, CON1, EX4, 6 brought up without being prompted: *"Understanding actually how important it is to protect the executive from the politics [...] if it is a newsworthy crisis, you know, you see the Chief executive being dragged off to talk to Government or the News or whatever, when actually his or her role should have been about actually managing the incident."* – [EX3].

3) Information Provided to the Board: When it comes to the type of information boards receive – or want to receive – audit results, penetration tests, and crisis simulations were described as the primary topics that should be brought to the boards' attention (CISO1,2,5; CON2,6; EX3,5; NED2): *"They [the board] are not involved in the direct exercise, but they get the output from the exercise and are interested in the outcome and the learnings from the exercise we run."* – [EX5]. This was followed by benchmarks and comparisons with other organizations (CISO1,2,3; EX1,6; NED1,2): *"[...] where are you in the industry type of figure, that the board will love because they will see, 'Okay, we are right here in maturity, and competitors are here'"* – [CISO1]. Vulnerabilities and (attempted) attacks were another topic for the board (CISO2,3; EX1,4,6; NED2): *"I know that in 2016 we saw 28 DDoS attacks on this firm of which we saw eight last year. Yeah. And the board will have seen that data and may not remember it but certainly, it will have been shared."* – [EX4]. The participants also mentioned incident reports or updates on data breaches (CISO2; EX1; NED1), as well as changes in maturity scores or KPIs (CISO2; EX1,4,5; NED4). Three CISOs (CISO1,3,4) would like to share more technical security details.

4) Partial Knowledge and Low Confidence: Some participants (CISO4; EX6; NED3,4) pointed out that NEDs lack a sufficient understanding of cybersecurity topics. Hence, they would be too shy to ask questions since they do not want to get embarrassed for their missing knowledge, e. g., *"They're perhaps just sometimes scared, that it's technology. I can't understand it, you know, it's a dark art it's a bunch of chaps in hoodies"* – [EX6]. Or *"When you start talking about, you know, you say cyber, you say climate, you say derivative, you say tech, you say firewall, you say, a list of words that your board members may not feel that they are experts in, and suddenly there, I think there is a confidence issue."* – [NED3]. Such low confidence directly impacts the board's ability to assess cybersecurity risk correctly and put the proper controls into place, as NED4 explained: *"Boards don't understand technology or security and so you can probably get away with an awful lot and you might say, 'Well, I didn't have the budget.'"* – [NED4]. Some CISOs took matters into their own hands. CISO3, for example, explained how they organized security training for the board so that they would finally be able to ask them appropriate questions: *"They [the NEDs] needed to be educated first before they could be challenging"* – [CISO3].

5) Cyber NEDs: While some participants stated that it would be good to have a dedicated NED with a cybersecurity background (e. g., *"Do you raise the knowledge level of the whole board or do you try to bring in an expert onto the board who can direct all the questions?"* – [NED3].), others disagreed and explained that in modern boards every NED would need to understand this topic: *"The board agrees with me that it is not right to have a single board member as the person who is the expert on cybersecurity. Every board member should know a little bit about it just as every board member should know a bit about everything, you know, and it is a collective activity."* – [NED1]. They then followed up and explained how their cyber knowledge shapes the work of the board: *"What is obvious in the last couple of months is they changed the people that are coming to the board meetings from the executive team. I am told [...] they are sending more technical people, and people who are more equipped to talk about how the program is being managed, and how programs are being organized and funded, because of the questions I am asking."* – [NED1]. NED2 explained that it would be hard to find a dedicated cybersecurity NED: *"The challenge, as I say, is you are highly unlikely to find a non-executive director who is expert in cybersecurity, and even if they were, how do they keep current, unless they are in a fulltime role and exercising a network?"* – [NED2].

6) Educating the Board: Only a few participants stated that boards would need to be educated on cybersecurity risks internally, either by NEDs with cybersecurity backgrounds or by the company's security specialists: *"I have taken the board through a, sort of, basic training program and how to ask the right sort of questions and what sort of things they should be thinking about from business perspective and then I am working with the company secretary now on a program to use [our] own technology people to give the board education about what cloud security is about."* – [NED1]. CISO2 explained that the board demanded some *cybersecurity manual* from them: *"We did something called the Cyber Series, which was basically the Audit Committee Chairman said to me, 'Can you write me a book on cyber?'"* – [CISO2].

Another mentioned topic was crisis simulations (also called *War Gaming*) for boards. While EX5 reported that their company's board only gets the "outcomes and learnings" (IV-B3), NED4 and EX6 explained direct board involvement in these scenario-based crisis simulations, *"[A] couple of boards actually do the war gaming thing, and I think it's helped. In fact, there was one board, which will not be named of course, which did actually go out to a third-party vendor and they in fact involved the NCSC as well [...] and I think they benefitted immensely"* – [EX6]. Additionally, CON3 suggested that NEDs should read security blogs to be updated on security topics: *"If people just read what was available on SANS NewsBites and a few other places, then they would do a lot better than they are currently doing."* – [CON3].

[2] https://ico.org.uk/about-the-ico/media-centre/talktalk-cyber-attack-how-the-ico-investigation-unfolded/, accessed February 4, 2025

7) Subcommittees: All participants explained that risk- and/or audit committees would do the board's heavy lifting of cybersecurity risk oversight. Such committees would be the primary place to discuss cybersecurity and question the CISO and CIO. CON2 explained why subcommittees would be so important for cybersecurity risk: *"They [overarching risk committees] are more effective than if they are just looking at their own particular single directorate. Quite often the biggest strength you have is to look across different directorates and to consider that a risk is not just a technical risk or a people risk."* – [CON2]. When it comes to the types and structure of those committees, only CISO5 and EX6 explained that they would have a dedicated *cyber committee* on an executive level: *"Some boards do have a separate cyber committee [...] especially some of the top FTSE 50 et cetera, tend to look at it separately and I think that is important for us to have a separate cyber committee [...] comprising people who understand this particular subject, I find that they're able to make a lot more progress."* – [CISO5]. And EX4 explained how multiple risk committees at different levels handle cybersecurity risks: *"There is a clear line through those four committees, yeah, from the most senior board level committee to the executive committee to my executive committee to the specialist committee in that area that are connected and the reports flow through. Obviously, there are different levels of granularity at each of those they are consistent in terms of the metrics that go to the board are not a parallel universe of metrics, they are a subset of the metrics that are used, you know, ultimately by the CISO to run and provide oversight of cyber security for the firm."* – [EX4]. NED3 stressed that nowadays, NEDs would have too many oversight tasks while only meeting a few times per year. Subcommittees would thus be the only way to find time to properly address cybersecurity: *"16 hours a year to oversee the entire operation of a company. It is not a lot of time, right? And you can be overwhelmed with material and just never have enough time to discuss everything. You know, so the committee structure allows the board to focus its time on, you know, bigger strategic issues and let the committees focus on the more narrow issues."* – [NED3].

Short Summary: Boards decide on cybersecurity risks through budgets, and their primary task is to ask the right questions to CISOs and executives (primarily in the risk/cyber subcommittees), but often won't because they fear their lack of cybersecurity knowledge will embarrass them. To get boards to ask the right questions, our participants presented two concepts: (I) bringing in cybersecurity experts and (II) educating the board on cybersecurity.

C. Boards & CISOs

The majority of our interviewed CISOs (CISO1,3,4) described their struggles to find the correct language and the right level of detail they should provide to the board: *"Sometimes I communicate something that I believe is right in the middle and will have very specific questions on very tiny parts of the communications, and sometime I will have the feedback that the communication was too detailed. So the biggest challenge, to sum up, is around what level of details do we need to communicate to a board. It has been an ongoing challenge all the time."* – [CISO1]. They further explained that the depth of questions varies massively between individual NEDs.

CISO5 described that other CISOs would lack social and communication skills. Hence, they would never get invited to speak directly at boards: *"If I meet a CEO and I say, 'As a matter of interest how often does your CISO brief the board?' I mean, some of them look absolutely horrified. They would not let their CISO within a hundred miles of the board. And that immediately tells you everything you need to know about the caliber of the person they have got."* – [CISO5]. EX3 described that they would not talk to the CISO because they would expect to get updates on security delivered directly by the CEO: *"All the boards I chair, or the boards I sit on, I never look to the IT or the CIO, I never look to them to give me a, 'Where are we on cyber?' I will always look to the chief executive to tell me where we are on cyber, and if he cannot answer that effectively we have got a problem."* – [EX3]. CISO2, on the other hand, summed up how they would work together with their executives to prepare the right information and the right way of presenting it to the board: *"In the run-up to any board meeting I will always have either one-on-one, or me and the CTO [Chief Technology Officer] will have a two-on-one with the Audit Committee Chair, and then we dive into much more detail there, and we also structure how are we going to run the meeting so that the right issues are teased out. So we are really, really transparent with the board. I think it is the only way to work because otherwise, they cannot fulfill their responsibility, and I partly see my job as helping them to do their job."* – [CISO2].

Here, something else shone through: if the board has a direct relationship with the CISO, the latter shapes the type of relationship, guides the conversations, and decides what security training the board should get. One would expect this the other way around – but due to a nagging unease about their lack of deep expertise – not just about cybersecurity, but IT generally (see Section IV-B4) – the CISOs seem to be the ones driving conversations and steering towards outcomes. CISO3 was especially dissatisfied with being asked general questions that did not challenge them and the company's security: *"Most boards are not very patient. And so I cannot even count on two hands how many times I have been asked, 'Are we going fast enough? Is the pace right? Is the budget right?'"* – [CISO3].

1) What to Talk About: Based on their personal backgrounds, our participants had different ideas about what topics should be discussed in a board session. NED4 explained that security would have such little time in the board schedule that the provided information would need to be on point: *"At the top, boards are like dashboards. So if you've got two minutes to talk about the security posture of a company at the highest level, you need a chart either on paper or on the [White-]board if they're doing it that way that says, 'Look, these five lines should all be up here, these two are going down, these three are going up and in order to bring the dashboard back into compliance we need to do these four things and it'll cost so many pounds - can you endorse that budget?'"* – [NED4]. In case of an incident, NED1 would like to get briefed on a more detailed level: *"What I would like to know is whether we have had any data losses, whether those data losses were material, whether they involved any, you know, privacy indications or, you know, PPI and those sorts* *of things and whether we have come close to contravening any regulations that might require us to call the ICO or to call the regulator, you know, and near misses."* – [NED1]. EX3 explained that technical topics should never be brought to the board: *"If you have a board conversation where someone is talking about what antivirus tool they are using, you have got a problem."* – [EX3]. Looking at the differences between NED1's and EX3's answers, CISO3's view on the topic of whether one should create a guide *on how to talk to boards* underlines the individuality of the boards' demands: *"Not really. It is just trial and error, isn't it?"* – [CISO3].

2) Reporting Line: In most of the organizations of our participants, the CISO would primarily report to the CIO and hence be part of the organization's IT. Direct board interaction was rare, but directly presenting reports to some form of risk committee was common, *"We have an executive risk committee that oversees also all of the big risks to the company, and all of my content would go through there before going on to any board or audit committee"* – [CISO2]. CISO2 also summed up what researchers and consultants have been arguing about now for years – where to place the CISO [60], [67], [68]: *"You have got the CISOs who think the CISOs should be part of the executive team and report to the CEO. You have got the people who do not want to sit in Technology or IT because they think it is a conflict, and then you have got people like me who want to sit in the place where you can get the most done and get the most attention. And I do not really care about my reporting line so much. I care about the access that I have got to make things happen and that people care, right."* – [CISO2].

Short summary: Boards and CISOs showed different risk abstraction levels, with CISOs viewing risks as more technical. To effectively communicate, our participants see a need to translate risks.

D. Cyberrisk: Not A Common Language

All CISOs, NED1, and NED2 were confident that *risk* should be the language used in any communication about cybersecurity between CISOs, boards, and executives. They explained that boards traditionally understand what risk is about. However, some participants, like CON2, were not so sure that organizational leaders would understand cybersecurity risks appropriately: *"They worry about risks holistically, where cyber risks are just one of the types of risks they are worried about. And some of the risks are closer to home and they are more likely to impact them. What boards do not necessarily understand is what the impact to them of a cyber risk is, and that is why having a way of quantifying the impact of a cyber risk I think would be beneficial."* – [CON2].

1) Risk Appetite: The term *risk appetite* for cybersecurity was mentioned by seven participants (CISO2,3; EX1-4; NED4). They saw it as a way to describe cybersecurity risk that needs to be compared to a previously set threshold of "acceptable risk". However, EX3 doubted that this concept would be well-known throughout the company: *"[...] the concept of risk appetite is not necessarily that well-known outside of the boardroom, or outside of Risk Committee, but it is absolutely key because it does come down to where do you spend your money, where do you spend your investment on protection and on litigation."* – [EX3]. Adding to the knowledge-gaps perceived by EX3, NED4 mentioned that *"Boards don't always understand risk appetite"* – [NED4]. EX2 gave a concrete example of what decisions around risk appetite could look like: *"Ransomware: What is the appetite? Is an organization going to pay with Bitcoins? Are we going to hold Bitcoins, as an organization, and be prepared to pay for that?"* – [EX2]. Besides EX2's example, the idea of how decisions based on appetite would look remained abstract, with CISO2 and CISO3 only mentioning the term as a side note.

2) Existing Risk Management Strategies: Even though cybersecurity was considered part of corporate risk management, cybersecurity risks were reported not to apply to current non-cyber risk management frameworks. Only three participants (CON1; EX2; NED3) saw parallels between the risk management strategies of their industry-specific risks and cybersecurity. NED3 first mentioned that they had difficulties measuring cybersecurity risks (among other operational risks): *"The ability to measure is something the financial services world is very comfortable with, and cyber and many operational risks do not easily fit into that framework."* – [NED3]. Later, they reported that they solved it by building upon an already existing financial risk management framework: *"I think there has been an evolution in financial services in terms of looking at cyber risk and how we think about it, using the framework that we all originally had around market and credit risk. Not to say, by any means, that the framework we had around market and credit risk was perfect, or is perfect today, because that is still evolving as well."* – [NED3].

Short Summary: Risk could be a common language spoken by NEDs, executives, and CISOs. But cybersecurity risk is not compared to traditional risk frameworks. The concept of comparing identified risks against a previously set risk appetite remained abstract.

E. Translation Service: Executives & CISOs

While the board advises and critically questions the executives' decision-making, the executives will decide on cybersecurity: *"They get to decide what is tolerable and what is not. How we then execute against that it definitely sits with the executive of the company, not the non-executives."* – [CISO2]. To effectively decide, EX2 described the difficulty of obtaining the correct information at an appropriate abstraction level: *"What makes it more effective - I think measuring the right things and reviewing the right things at the right level is very important, so a good dashboard which describes risks in all its aspects and enables management decisions to be made in a timely and effective manner."* – [EX2]. They then added: *"One of the risks is that organizations or companies can ask for more and more detail, more and more data to avoid making decisions, which is one end of the spectrum. The other end of the spectrum is that they do not have any data and therefore do not understand the risks that apply within their organization."* – [EX2]. To get to the *correct level of detail*, the language of risk – which implies the need to translate cybersecurity risks into more abstract, general risks – was brought up during our interviews (see Section IV-D).

1) Working Together to Translate Cybersecurity: CISOs consider executives to be part of their communication channel with the board. EX3 described this channel as necessary since cybersecurity is not a risk that should be delegated to the CISO or CIO and left alone: *"I think too often the executive delegates to the CISO or the CIO, and they go off into a dark room and try and fix it, which of course they cannot. So I think many non-executives in that type of company will become increasingly alarmed at the lack of transparency and the lack of business articulation of the risk."* – [EX3]. To achieve this transparency, the mentioned CISOs and CIOs would need to be able to communicate these risks in an, from the perspective of the board, understandable manner: *"I think it is down to the responsibility of the CIO and the CISO to make sure that they are reporting to the board in a language the board can understand, in business language."* – [NED1]. For example, CISO1 described that their CFO was presenting for them at the board: *"What I do is I prepare the material for the CFO to present to the board. And that is another challenge, is that the CFO is not, is not an IT person. So I need to give him the material and he is the one communicating to the board. Then he is getting questions, feedback, and inputs, then I am getting afterwards. I do not have direct communication."* – [CISO1]. This CFO then would translate the information to be fit for presentations at the board level: *"I think it works really well because he understands and he manages to put that in the bigger perspective and translate that, removing the IT, geeky world and concept out of it"* – [CISO1].

Short Summary: To translate the technical risks of the CISO's cybersecurity department to be fit for presentations at the board level, the executive the CISO is reporting to may be able to assist.

F. External Influences on Cybersecurity Risk

Regulators, consultants, security agencies, auditors, and investors all played a role in shaping the board's cybersecurity risk agenda, which we explore in this section.

1) Regulatory Influence on Cybersecurity Risk: CISO2 and CISO3 described regulations as *selling-points* to receive sufficient funding at board- and executive-level:*"Agencies and regulators can really help you land the message about the threat, why it is important, what type of things would they expect the company to be focused on. And I think if it is somebody who is struggling to get access to funding, for example, it could be a really good way of helping that decision-making"* – [CISO2]. CISO3 directly described that they would be much more powerless without regulations: *"Regulation elevates the profile with boards, and I think that is healthy because else it could get pushed down and you might lose traction."* – [CISO3].

Besides using regulation as a selling point, two schools of thought could be observed during our interviews: (I) Regulatory bodies do not have a big impact on corporate cybersecurity besides acting as an *information source*: *"They [regulatory bodies] are good sources of information and insight. I do not think there is anybody that is directive. I think we are self-directed."* – [EX4]. (II) Corporate cybersecurity is only focussing on regulatory requirements, also described as a *tick-box approach*: *"I essentially went to the head of compliance and risk management [...] and I said, "Can you describe how you do your group risk?" [...] And to cut a long story short, he said, "We have a basis book, and the basis book lists our regulations, and our risks are that we do not meet our regulations." "And?" "And what? And that is it.""* – [CON3].

Seven participants mentioned security agencies and regulatory bodies as a source of up-to-date information. NEDs (NED3,4) and executives (EX2,4,6), in particular, saw those agencies and regulatory bodies as a man-in-the-middle to share aggregated and anonymized security information that companies would not share directly: *"They do it one-on-one to the security service or somebody, but they wouldn't do it to their competitors."* – [NED4]. CISO3 further stated: *"You can share, you know, anonymized conversations, and I think that is important for the board to hear from the likes of the NCSC themselves as opposed to through myself. It carries just more weight, and obviously, they will have more depth of the experience as well. So, I think they are really important because it just shows you what can really happen out there, even if it is not happening to you."* – [CISO3]. They also wished for more information sharing by the national cybersecurity agency: *"I do think they could do a lot more in sharing what they know."* – [CISO3].

2) External Auditing: While internal auditing might be less expensive, according to NED4, boards seem to demand external audits to avoid conflicts of interest: *"You could argue that your team should be looking after your company. But it becomes a conflict of interests then. In other words to your point, you definitely need an external trusted pen test company if it's penetration testing we're talking about."* – [NED4]. Some participants viewed external auditing as a way to ensure and gain a different perspective on corporate cybersecurity: *"I would say that third-party review and auditing if you will, I think that should be an integrated part of any cybersecurity. Because you only see things with your own perspective, right? So you only know what you know, and it is always good to have external independent eyes to look you over the shoulder."* – [EX5]. Additionally, similar to regulatory bodies, external audits can also give insights into where the company's cybersecurity is better or worse compared to their competitors: *"It is a significant project [getting audited] and it provides you where are you in the industry type of figure, that the board will love."* – [CISO1].

However, executives also shared their distrust in the professionalism of auditors. This distrust was most common when participants stated one of the "Big Four" consulting agencies as auditing body: *"The financial services sector have what they call Section 166 inquiries*[3]*, where they will drop a skilled person, which I always laugh at because I mean, you know, it is someone from PwC; he used to work for a bank, you know. He is no more skilled than anybody."* – [EX3].

3) Consultants: We found our participants to be skeptical about consultants. They explained that managing cybersecurity risks can not be done by getting a consultant in and buying or implementing their recommendations once. Even CON3, a consultant themselves, criticized how others would exploit an information asymmetry when they advise senior leaders: *"They bring in a contractor, and the contractor says, 'You need this procedure. You need that guard here, and you need to change that control system, and then you are good to go*

[3] Section 166 is calling for an *skilled person* to provide a report. https://handbook.fca.org.uk/handbook/EG/3/3.html

for the next five years or two years.' And what they want is the same for cybersecurity. And my message is, and this is the difficult message to get to the board, my message is, 'No, I am sorry. You are going to have to maintain some competence to understand your risks and how those risks will change.' And the boards just do not want to hear that." – [CON3]. EX3 extended on this point by adding that it is the board's job to challenge cybersecurity, and thus outsourcing it to a consultant is an "abdication of duty".

4) Investors' focus on Cybersecurity: During the interviews, our participants were asked whether potential investors would be interested in the company's current cybersecurity state and what investors should look for to determine the maturity of the cybersecurity program. While CISO2, who has been presenting to investors for the last five years, has observed a positive trend in investor interest (*"I have seen a big uptake over the last three years actually in interest from investors."* – [CISO2].), most participants reported that they were never asked about cybersecurity at investor presentations: *"I sit through quarterly investor presentations, and I have never heard a question about it. Which is surprising, now you mention it."* – [NED2]. NED3 stated that cybersecurity risk is such a specific (maybe small) topic that investors really might not be interested in such details: *"I mean I would be amazed if any investor ever asked questions about cybersecurity because, you know, it is one of many, many things that a company manages."* – [NED3]. NED4 even doubted that this would be an appropriate question for investors: *"Well the first question is would a serious investor even think of asking that question?"* – [NED4].

Short summary: Regulations helped to bring cybersecurity risk to boards' attention. However, some participants feared a *ticking boxes* approach. Our participants wished for more process-oriented regulatory frameworks and results-sharing of those assessments. Investors were described as rarely looking at cybersecurity risks before their investments.

V. Discussion

Reflecting on the results of the study we carried out with UK-based boards, we discuss our findings and answer our research questions.

A. Q1: Cybersecurity Risk Decision-Making

All our participants agreed that cybersecurity risk is a topic in most boardrooms. But there is no in-depth engagement: Most board decisions are based on (very short) cybersecurity reports from those seen to be experts – the CISO, CIO, external auditors, or, in rare cases, the CEO. The vast majority of board decisions on cybersecurity were to approve the budget requests from the CISO or executives (IV-B). While *risk apptetite* was used by several participants, nobody explained the term or the process the board went through to decide the appropriate level for cybersecurity. Without specific knowledge in the boardroom, the process was *delegate and trust the experts*, similar to how in the past decisions about general IT were made: *Just put an IT guy and enough money on it, and it will be solved*. As IT moved to the core of many businesses, this changed to a more considerable board involvement in concrete IT decisions [69], [22], [23]. Our results indicate that for cybersecurity, this is not yet the case for all large organizations.

While we agree with most of our participants that boards should not make detailed technical decisions, such as which antivirus tool to buy (IV-C1), cybersecurity risks should not be abstracted through budgets alone. Strategic and concrete *risk-appetite* board decisions could e. g., be made around risks concerning data security (in which countries and at servers of which partner organizations should data be stored?) or redundancy (what would be the maximum tolerable level of an outage due to a cyber attack?). Such decisions would link budgeting with a clear strategy that could be co-designed by NEDs and executives. The information the board is provided with already is more diverse than the decisions they ultimately make (IV-B3).

We also got some insights into what cybersecurity means to boards: (I) It is perceived as part of IT (IV-C2), and in these organizations, security and the CISO were still a part of the IT department making it more challenging to put non-IT changes in place. (II) Cybersecurity is about confidentiality. The loss of (personal) data is the primary scenario our participants want to prevent (IV-C1). Here, cybersecurity is mainly seen through one specific aspect rather than as a complex topic. In 2007, Flechais et al. [70] identified the problem of non-security-experts setting cyber security equal to confidentiality and leaving out other aspects. The reasons seem to be strictly driven by regulation and fines organizations have to fear in case of an incident – something already described by recent studies [29], [71]. On the plus side, this shows that regulators (or, more concretely, legislation) can steer how boards perceive and talk about security by setting appropriate standards and matching fines – as the GDPR brought cybersecurity risks to boards' attention [27].

Board meetings offer little space for cybersecurity activities, and NEDs are only paid for a limited number of days [72]. They are unlikely to have the time to do deep dives on cybersecurity. However, continuously educating and training board members – through micro-learning sessions around the meetings themselves or at informal NED roundtable events – would be necessary to probe the decision-making on cybersecurity more detailedly than just asking: "Do you've got enough budget?". Multiple participants suggested this – as did other scholars [26], [32] and cyber agencies [7], [21]– in the form of cyber crisis simulations or war gaming, dedicated training courses, or even handbooks (IV-B6).

War gaming was often mentioned as the go-to training for boards. However, one NED pointed out that this was a misguided approach to raising awareness and a waste of time: board members should not be involved in crisis decision-making. In these situations, the executives have to "fly the plane", a process other board members should not meddle in. Instead, they should "create time and space for the executives" (IV-B2). Short but continuous training to increase the ability to challenge the CISO's decisions beyond asking questions about budgeting was reportedly promising and also demanded by some board members. However, to avoid conflicts of interest, these training should not be provided exclusively by the CISOs themselves.

In organizations that have created structures (sub-

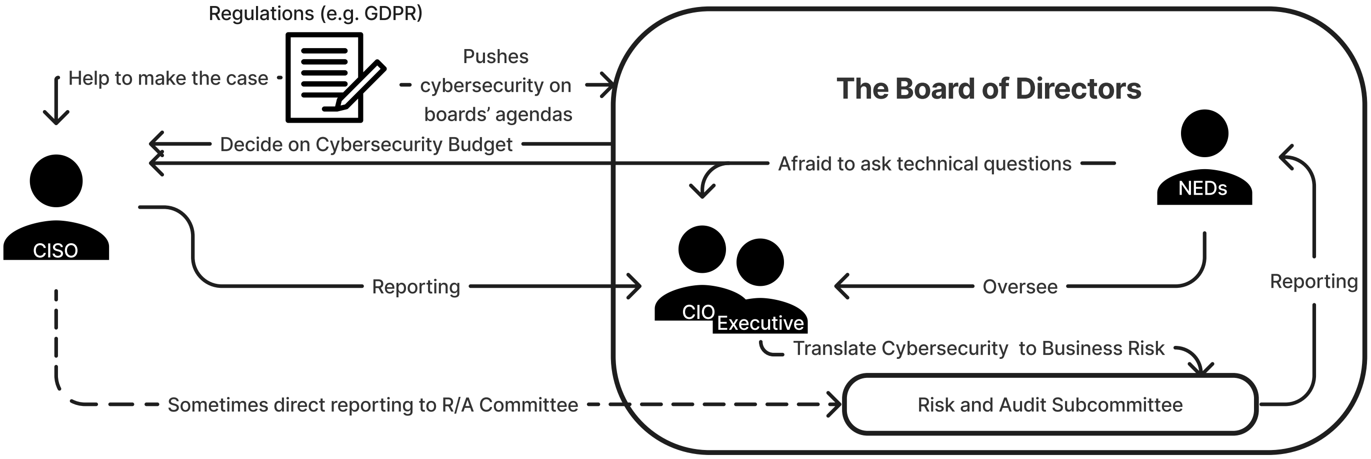
Regulations (e.g. GDPR)
Help to make the case
Pushes cybersecurity on boards' agendas
The Board of Directors
Decide on Cybersecurity Budget
Afraid to ask technical questions
NEDs
CISO
Reporting
Oversee
Reporting
CIO
Executive
Translate Cybersecurity to Business Risk
Sometimes direct reporting to R/A Committee
Risk and Audit Subcommittee

Fig. 2. Key relationships that form cybersecurity risk decisions at the board.

committees) for dealing with risks, the decision process becomes more distributed (IV-B7). A few organizations in our sample had dedicated cybersecurity risk committees. In others, the general risk and audit committee dealt with cybersecurity risk as one topic among many. The committees – often chaired by an NED – hear reports from executives (like the CEO or CIO) or the CISOs, rate risks, evaluate progress, condense available information for the board, and make recommendations. While the committee does not decide, its findings and recommendations are usually followed. Interestingly, previous studies did not distinguish whether CISOs would report to the board as a whole [41], [2], or *just to a subcommittee*. Our results indicate that most CISOs might never speak in front of the board but in front of subcommittees. This severely affects the level of detail they can hope to bring forward.

B. *Q2: Stakeholder Influence*

Figure 2 summarizes critical relationships with other stakeholders that shape the board's cybersecurity risk decisions. One would suspect that the board – at the very top of an organization – would have the power and self-determination to decide on cybersecurity risk strategies on a level of detail they dictate. However, our results show that often the CISOs set the agenda and make cybersecurity decisions, and they (or the executives they report to) determine which information they want to report to the board without much input from both NEDs and other Executives. This has multiple reasons:

(I) Most board members do not have cybersecurity expertise. This is problematic when they fail to challenge reports and recommendations because they fear basic questions might reveal their lack of knowledge (IV-B4) leading to not fulfilling their oversight role. This leads to a power imbalance where CISOs (and CIOs) can decide what they want to report to the board. Some participants even reported that the CISOs would train the board about cybersecurity, directly influencing the board's oversight function. While CISOs might not see themselves in a position of power towards the board [3], [2], they are – even if they are a type of person that no NED wants to see in front of the board (IV-C). They can unfold their power indirectly by silently deciding what information reaches the executives.

The difference from other risks (like classic credit risk) is that multiple board members will feel knowledgeable enough to be unafraid to ask tough questions. In the few cases where NEDs with cybersecurity risk knowledge were part of the board (IV-B5), the power shifted from the CISOs towards those single NEDs. This might change in the next generation when the role of CISOs gets executive status and thus board member. Regulators and scholars [73], [74] demand such IT and cybersecurity experts on every board. Our participants had mixed viewpoints about this, with some highlighting that if boards had such experts, those would carry the whole oversight alone (IV-B5). We agree that this will hardly diminish the power imbalance. However, at least US regulators seem confident that a person with explicit cybersecurity knowledge should be part of the board: Following a US Securities and Exchange Commission proposal, every US corporation traded on the stock market might soon be forced to recruit a CISO for their board.[4] The already approved new EU NIS2 directive[5] might have a similar impact since it states that "management bodies of essential and important entities are required to follow [cybersecurity] training".

(II) Risk is not equal to cybersecurity risk. While our participants agreed that the CISOs need to talk in the *language of risk* – as other studies have already shown that CISOs need to find appropriate language [51], [2] – their risk vocabulary might not be compatible. The problem that shines through our results is that NEDs and executives do not know what cybersecurity risk is, how to estimate cybersecurity risks, and how to set *risk appetite* in this realm. Neither can CISOs alone translate their cybersecurity risks into more general terms of risk without knowing about other company risks. The result is that cybersecurity decisions are abstracted by setting a certain level of security budget on which they agree. This security budget our participating CISOs had to work with did not seem well estimated since they reported that their budget was either underestimated or overestimated. This idea of *give cyber enough money and the problems will go away* is in harsh

[4] The SEC Is About To Force CISOs Into America's Boardrooms: https://www.forbes.com/sites/bobzukis/2022/04/18/the-sec-is-about-to-force-cisos-into-americas-boardrooms/amp/, accessed February 4, 2025.

[5] NIS2 Directive: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive, accessed February 4, 2025

contrast to other risk decisions the leaders are involved in, e. g., when they directly decide to invest in new markets or not.

(III) Regulations (like the GDPR) help to bring cybersecurity risk to boards' attention (IV-F1) – as previous studies already discovered [27]. Their effects are two-fold: (I) The topic *automatically* made it on boards' agendas (despite the CISOs deciding on what exactly to talk about). (II) CISOs have an easier time getting the resources they need just by referring to regulations.

As an external (independent) board member, NEDs rely on two sources of information: (I) Experience reports from peers and benchmarks against the cybersecurity risk performance (success of their strategy in terms of investments and incidents) of other organizations – a primary source of information for boards (IV-B3). (II) External Audits (IV-F2). However, some participants had doubts about the independence and quality of such audits since they were often delivered by the same companies that would try to acquire consulting contracts with the board.

Interestingly, investors (shareholders) do not play any role in boards' handling of cybersecurity risks. While boards of larger companies – elected by those shareholders – typically aim to increase the company's value for shareholders, in the experience of our participants, cybersecurity risk is seldom a topic the shareholders ask about. Currently, there is no pressure on the board from shareholders. This was even true for those organizations that had already suffered losses through cybersecurity incidents with public news coverage.[6]

C. Learnings For Practitioners

Cybersecurity risk is handled *informally* by the board, unlike traditional risks where it is regulated which specific information needs to be reported to the board. While companies are subject to different cybersecurity regulations, those do not state what information needs to reach the boards. For example, even the EU's new NIS2 Directive for critical infrastructure does put the board of directors (or *management bodies* how they call it) in charge of oversight of cybersecurity risks. They shall maintain a *high level of awareness*, *monitor the efforts*, and *approve whole risk strategies* [75]. But again, there are no concrete metrics to test against, and what and how information should flow through the hierarchies is not defined. We suggest that it should be the task of future regulations to set baselines for information that boards need to get, e. g., investments vs. incidents. This would shift the power imbalance we discovered.

1) Incident Disclosure Through Regulators: Our study shows that regulators considerably impact companies' boards' work with cybersecurity. This is not only through new laws but also through the (anonymized and aggregated) incident reports that those agencies publish that serve as industry benchmarking for the boards. However, such benchmarking is often limited to what organizations want to disclose – in most cases, nothing as long as they are not forced through a privacy law (like the GDPR) or critical infrastructure regulations [76], [77]. Hence, those reports are often not applicable to specific industries – and with the other primary source of public incident reports available coming from security vendors and consultants that have an information advantage over their customers [78], the number of unbiased, objective reports is further limited. We suggest extending the disclosure requirements beyond data privacy and critical infrastructure organizations. Those disclosures should stay anonymous, but the data can be aggregated and publicly disclosed. The EU has been proven to be a powerful legislative body and could initiate such efforts that could be adapted in the UK.

2) NEDs as Leaders: Most participants were certain that it would be the NEDs' job to have the executives' back in a crisis. We agree. This includes that a NED should create time and space for their executives in case of severe cybersecurity incidents, as the executives would be fully involved in direct crisis management. Such crisis management requires planning and crisis simulations. Different leaders' roles must be clarified beforehand, especially who will make which decisions in such cases. However, it is unrealistic for NEDs to participate in war games and simulations. They need to be told what their role would be in a crisis, or more concretely, the executives should suggest the roles the board would take over, and then the board decides which NED to appoint to which position.

Also, NEDs were referring to the example of the TalkTalk CEO described in IV-B2, indicating being afraid to be exposed when asking questions. However, we see a clear difference between publicly exposing and asking novice questions at the board. We follow Sheryl Sandbergs' idea of *lean in* [79] that states that great leaders should never lean back but actively engage in discussions - no matter the social costs. Being afraid of other board members' opinions should not be an excuse for NEDs not to challenge executives and CISOs. Despite consultants recommending cybersecurity training for NEDs, available trainings are time-consuming and generic. Thus, NEDs prefer to obtain knowledge from their peers through roundtables or similar events. This knowledge gap might also naturally shrink in the upcoming years as more CISOs and CIOs become senior enough to be offered NED positions.

Further, we propose that it is time for the NEDs and executives to make sure they support their CISO with non-technical aspects of their job by, e. g., leading by example when it comes to cybersecurity behavior, calling out managers who do not encourage their staff to adopt security behaviors, and identifying existing roles and resources that can work with CISOs to reduce friction between business and security, develop communication strategies, campaigns, and training materials for different business areas.

3) Building Cybersecurity Risk Subcommittees: A dedicated cybersecurity risk subcommittee should be implemented to close the gap between traditional (non-cybersecurity) risk management frameworks and cybersecurity. This subcommittee can act as a bridge between the technical cybersecurity departments and management. Detailed monitoring of risks and aggregating risks to a current state that might be able to answer the question "Where are we on cyber?" should happen at this subcommittee. To do so, the subcommittee should consist of the CISO, at least one NED, employees from the non-cybersecurity risk subcommittees, and (on-demand) further security experts. This mixture of different domain experts combined with an NED can, over time, prepare the CISO to

[6] For anonymity reasons, we cannot name the specific organizations or incidents participants referred to.

translate and distill the most pressing cybersecurity risks to be presentable at the board by the CISO.

D. Learnings For Researchers

Previous research with CISOs has shown they don't have the time to stay on top of academic cybersecurity developments [2]. It is even more unlikely that NEDs and executives keep abreast with cybersecurity publications(IV-B6). For them, decisions are always in the context of business and business risk – so learning about cybersecurity risks in isolation is not helpful. As a research community, we should consider how we might digest and disseminate our results and effectively and efficiently translate them to *business language*.

Previous research has already studied some board members in isolation, e. g., NEDs [29]. In contrast, we conducted a study with a multitude of different roles, namely NEDs, executives, consultants, and CISOs. This multi-perspective view on the topic led us to novel findings, such as the power imbalance between NEDs and CISOs/CTOs that can steer communication by only providing specific (beneficial) data. Based on our experience, we generally advise such multi-stakeholder studies wherever multiple stakeholders influence cybersecurity processes.

1) Cybersecurity Risk Management: Our participants described different approaches to processing cybersecurity information for boards, with mixed results – CISO3 even called it *Trial and Error* (IV-C1 and IV-E1). A good starting point could be investigating the applicability of existing risk management frameworks (such as for financial or physical risks) to cybersecurity risks. Additionally, the question of who should be responsible for translating remains. The person or committee must have (deep) technical knowledge and a broad understanding of the companies' business and (non-cybersecurity) risks. Further, in recent years, the research on security metrics – including those that are supposed to be relevant to the management – has been growing [80], [81], [82]. However, those metrics were developed by cybersecurity experts, but there has been no research to validate how helpful they are to boards – or what metrics they consider pertinent. For example, boards might solely want to see financial losses vs. revenue of an investment rather than any numbers suggested by frameworks, like click rates in simulated phishing exercises. Within most companies included in this work, the CISOs set the agenda and decide what to present (through executives) at the board level (IV-C).

2) Recruting C-Level Participants: More studies about cybersecurity topics with C-level participants are needed to understand their individual and collective decision-making. This group of participants is hard to recruit. Still, we found that government agencies responsible for cybersecurity (like the NCSC in the UK, or the German BSI), nowadays have gatherings of such top-level leaders. Based on our own experience, we advocate brokering connections between trusted researchers and top-level leaders for further studies. Once such trust has been built and benefits emerge, more scientific studies in ecologically valid contexts, such as boardroom observations or, tracking cybersecurity risks from identification to remediation, could be carried out.

VI. Conclusion

We interviewed $n = 18$ UK-based top-level leaders, giving us previously unknown insights into how cybersecurity is decided at the highest organizational level. While cybersecurity risks are increasingly present on boards' and their subcommittees' agendas, we found multiple indicators that they are not appropriately addressed. NEDs are too shy to ask the right questions to their executives and CISOs because they lack technical knowledge. CISOs must translate their cybersecurity risks into a more business-focused language to get challenged on cybersecurity topics. This need to abstract the complexity of cybersecurity risks into more general risks creates a power imbalance since the CISOs could decide which topics to present and shine light on. The board's role of overseeing the companies' key risks – which cybersecurity risks were reported to be part of – cannot be thoroughly carried out this way. Future research should quantify the problems identified in this paper through larger-scale studies with senior leaders in different regions. Recruitment facilitated by government agencies can be key to realizing such studies.

Acknowledgments

Thanks to all our participants for their time, trust, and valuable insights. Thanks to Simon Parkin for helping with the interview guide and code book, and Diego Sempreboni for supporting, organising, and conducting the interviews. Thanks to Markus Schöps, Felix Reichmann, and Marco Gutfleisch for proofreading. The project was funded by the UK NCSC and Lloyds Register Foundation, as well as the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC 2092 CASA – 390781972, and also by the PhD School "SecHuman - Security for Humans in Cyberspace" by the federal state of NRW, Germany.

References

[1] National Cyber Security Centre UK, "NCSC: Annual Review 2023," 2023.

[2] J. Hielscher, U. Menges, S. Parkin, A. Kluge, and M. A. Sasse, ""Employees who Don't accept the time security takes are not aware Enough": The CISO view of Human-Centred security," in *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 2311–2328.

[3] D. Ashenden and A. Sasse, "CISOs and organisational culture: Their own worst enemy?" *Computers & Security*, vol. 39, pp. 396–405, 2013.

[4] R. Klimoski, "Critical success factors for cybersecurity leaders: Not just technical competence," *People and Strategy*, vol. 39, no. 1, p. 14, 2016.

[5] W. Baker, M. Goudie, A. Hutton, C. D. Hylender, J. Niemantsverdriet, C. Novak, D. Ostertag, C. Porter, M. Rosen, B. Sartin *et al.*, "2011 data breach investigations report," 2011.

[6] German Federal Office for Information Security, "The State of IT Security in Germany 2023," 2023.

[7] National Cyber Security Centre UK, "Cyber Security Toolkit for Boards," 2023. [Online]. Available: https://www.ncsc.gov.uk/files/NCSC_Cyber-Security-Board-Toolkit.pdf

[8] E. F. Fama and M. C. Jensen, "Separation of ownership and control," *The journal of law and Economics*, vol. 26, no. 2, pp. 301–325, 1983.

[9] SEC, "Federal Register Commission Statement and Guidance on Public Company Cybersecurity Disclosures," 2018.

[10] S. Schinagl and A. Shahim, "What do we know about information security governance? "from the basement to the boardroom": towards digital security governance," *Information & Computer Security*, vol. 28, no. 2, pp. 261–292, 2020.

[11] R. A. Rothrock, J. Kaplan, and F. Van Der Oord, “The board’s role in managing cybersecurity risks,” *MIT Sloan Management Review*, vol. 59, no. 2, pp. 12–15, 2018.

[12] L. Georg-Schaffner and E. Prinz, “Corporate management boards’ information security orientation: an analysis of cybersecurity incidents in dax 30 companies,” *Journal of Management and Governance*, vol. 26, no. 4, pp. 1375–1408, 2022.

[13] M. Lipton, D. A. Neff, A. R. Brownstein, S. A. Rosenblum, A. O. Emmerich, and S. L. Fain, “Risk management and the board of directors,” *Bank and Corporate Governance Law Reporter*, vol. 45, no. 6, pp. 793–799, 2011.

[14] E. L. Opitz, “Cybersecurity for the board of directors of small and midsized businesses,” *Board Leadership*, vol. 2018, no. 159, pp. 4–5, 2018.

[15] N. Lankton, J. B. Price, and M. Karim, “Cybersecurity breaches and the role of information technology governance in audit committee charters,” *Journal of Information Systems*, vol. 35, no. 1, pp. 101–119, 2021.

[16] S. Héroux and A. Fortin, “Board of directors’ attributes and aspects of cybersecurity disclosure,” *Journal of Management and Governance*, vol. 2024, no. 1, pp. 1–46, 2022.

[17] J. L. Higgs, R. E. Pinsker, T. J. Smith, and G. R. Young, “The relationship between board-level technology committees and reported security breaches,” *Journal of Information Systems*, vol. 30, no. 3, pp. 79–98, 2016.

[18] J. B. Price and N. Lankton, “A framework and guidelines for assessing and developing board-level information technology committee charters,” *Journal of Information Systems*, vol. 32, no. 1, pp. 109–129, 2018.

[19] L. Caluwe and S. De Haes, “Board engagement in it governance: Opening up the black box of it oversight committees at board level,” 2019.

[20] M. Ramírez, L. Rodríguez Ariza, M. E. Gómez Miranda *et al.*, “The disclosures of information on cybersecurity in listed companies in latin america—proposal for a cybersecurity disclosure index,” *Sustainability*, vol. 14, no. 3, p. 1390, 2022.

[21] L. Clinton, A. Marx, K. Swafford, and D. Sandlin, “NACD & Internet Security Alliances’ Directors Handbook on Cyber-Risk Oversight,” 2023.

[22] M. Ashraf, P. N. Michas, and D. Russomanno, “The impact of audit committee information technology expertise on the reliability and timeliness of financial reporting,” *The Accounting Review*, vol. 95, no. 5, pp. 23–56, 2020.

[23] E. L. Valentine and G. Stewart, “The emerging role of the board of directors in enterprise business technology governance,” *International Journal of Disclosure and Governance*, vol. 10, pp. 346–362, 2013.

[24] A. Bonime-Blanc, “A strategic cyber-roadmap for the board,” 2016.

[25] N. E. Vincent, J. L. Higgs, and R. E. Pinsker, “Board and management-level factors affecting the maturity of it risk management practices,” *Journal of information systems*, vol. 33, no. 3, pp. 117–135, 2019.

[26] N. Smaili, C. Radu, and A. Khalili, “Board effectiveness and cybersecurity disclosure,” *Journal of Management and Governance*, vol. 2022, no. 1, pp. 1–23, 2022.

[27] A. Klein, R. Manini, and Y. Shi, “Across the pond: How us firms’ boards of directors adapted to the passage of the general data protection regulation,” *Contemporary Accounting Research*, vol. 39, no. 1, pp. 199–233, 2022.

[28] PWC, “How your board can better oversee cyber risk,” 2018.

[29] M. Gale, I. Bongiovanni, and S. Slapnicar, “Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead,” *Computers & Security*, vol. 121, p. 102840, 2022.

[30] E. McFadzean, J.-N. Ezingeard, and D. Birchall, “Perception of risk and the strategic impact of existing it on information security strategy at board level,” *Online Information Review*, vol. 31, no. 5, pp. 622–660, 2007.

[31] S. Wallace, K. Green, C. Johnson, J. Cooper, and C. Gilstrap, “An extended toe framework for cybersecurity adoption decisions,” *Communications of the Association for Information Systems*, vol. 47, no. 2020, p. 51, 2021.

[32] C. Abraham, D. Chatterjee, and R. R. Sims, “Muddling through cybersecurity: Insights from the U.S. healthcare industry,” *Business Horizons*, vol. 62, no. 4, pp. 539–548, 2019.

[33] F. Rashid, “Nyse survey examines cybersecurity in the boardroom,” 2015.

[34] B. Shreeve, J. Hallett, M. Edwards, K. M. Ramokapane, R. Atkins, and A. Rashid, “The best laid plans or lack thereof: Security decision-making of different stakeholder groups,” *IEEE Transactions on Software Engineering*, vol. 48, no. 5, pp. 1515–1528, 2020.

[35] C. Radu and N. Smaili, “Board gender diversity and corporate response to cyber risk: evidence from cybersecurity related disclosure,” *Journal of business ethics*, vol. 2021, no. 1, pp. 1–24, 2021.

[36] M. M. M. Mazumder and D. M. Hossain, “Voluntary cybersecurity disclosure in the banking industry of bangladesh: does board composition matter?” *Journal of Accounting in Emerging Economies*, vol. 13, no. 2, pp. 217–239, 2023.

[37] C. Shayo and F. Lin, “An exploration of the evolving reporting organizational structure for the chief information security officer (ciso) function,” *Journal of Computer Science*, vol. 7, no. 1, pp. 1–20, 2019.

[38] Erastus Karanja, “The role of the chief information security officer in the management of IT security,” *Inf. Comput. Secur.*, vol. 25, pp. 300–329, 2017.

[39] D. Whitten, “The chief information security officer: An analysis of the skills required for success,” *Journal of Computer Information Systems*, vol. 48, no. 3, pp. 15–19, 2008.

[40] Julia H Allen, Gregory Crabb, Pamela Curtis, Brendan Fitzpatrick, Nader Mehravari, and David Tobar, “Structuring the Chief Information Security Officer Organization,” 2015.

[41] V. Hooper and J. McKissack, “The emerging role of the ciso,” *Business Horizons*, vol. 59, no. 6, pp. 585–591, 2016.

[42] M. Bartsch, “Woher nehmen, wenn nicht stehlen – oder wo haben Sie Ihren CISO her? (German),” in *Cybersecurity Best Practices*, M. Bartsch and S. Frey, Eds. Wiesbaden: Springer Fachmedien Wiesbaden, 2018, pp. 261–269.

[43] M. Goodyear, H. T. Goerdel, S. Portillo, and L. Williams, “Cybersecurity Management In the States: The Emerging Role of Chief Information Security Officers,” *SSRN Electronic Journal*, vol. 2023, no. 1, pp. 1–44, 2010.

[44] S. B. Maynard, M. Onibere, and A. Ahmad, “Defining the Strategic Role of the Chief Information Security Officer,” *Pacific Asia Journal of the Association for Information Systems*, vol. 2018, no. 1, pp. 61–86, 2018.

[45] A. B. Anderson, A. Ahmad, and S. Chang, “Competencies of cybersecurity leaders: A review and research agenda,” *ICIS 2022 Proceedings*, vol. 2022, no. 9, 2022.

[46] T. Caulfield and D. Pym, “Improving security policy decisions with models,” *IEEE Security & Privacy*, vol. 13, no. 5, pp. 34–41, 2015.

[47] R. Singh, P. Mulgund, and S. D. Smith, “Exploring the evolving balance of power between cisos and cios: A qualitative perspective,” *AMCIS 2024 Proceedings. 6.*, 2024.

[48] T. Moore, S. Dynes, and F. R. Chang, “Identifying how firms manage cybersecurity investment,” *Available: Southern Methodist University.*, vol. 32, 2015.

[49] E. Albrechtsen and J. Hovden, “The information security digital divide between information security managers and users,” *Computers & Security*, vol. 28, no. 6, pp. 476–490, 2009.

[50] L. Reinfelder, R. Landwirth, and Z. Benenson, “Security Managers Are Not The Enemy Either,” in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI ’19*, S. A. Brewster, G. Fitzpatrick, A. L. Cox, and V. Kostakos, Eds. New York, New York, USA: ACM Press, 2019, pp. 1–7.

[51] J. Da Silva, “Cyber security and the Leviathan,” *Computers & Security*, vol. 116, p. 102674, 2022.

[52] J. Da Silva and R. B. Jensen, “”cyber security is a dark art”: The ciso as soothsayer,” *Proc. ACM Hum.-Comput. Interact.*, vol. 6, no. CSCW2, nov 2022.

[53] S. Parkin, A. van Moorsel, P. Inglesant, and M. A. Sasse, “A stealth approach to usable security: Helping it security managers to identify workable security solutions,” in *Proceedings of the 2010 New Security*

Paradigms Workshop, ser. NSPW '10. New York, NY, USA: Association for Computing Machinery, 2010, p. 33–50.

[54] T. Fitzgerald and M. Krause, "CISO leadership: Essential principles for success," 2007.

[55] M. R. Lowry, A. Vance, and M. D. Vance, "Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity," *SANS*, vol. 2021, no. 1, 2021.

[56] D. Death, "The CISO Role within US Federal Government Contracting Organizations: A Delphi Study," Ph.D. dissertation, Capella University, 2021.

[57] G. Armbruster, J. Whittington, and B. Endicott-Popovsky, "Strategic Communications Planning for a CISO: Strength in Weak Ties," in *Journal of The Colloquium for Information Systems Security Education*, vol. 2. Severn: CISSE, 2014, p. 10.

[58] E. Karanja, "The role of the chief information security officer in the management of it security," *Information & Computer Security*, vol. 25, no. 3, pp. 300–329, 2017.

[59] J. Hielscher, M. Schöps, U. Menges, M. Gutfleisch, M. Helbling, and M. A. Sasse, "Lacking the tools and support to fix friction: Results from an interview study with security managers," in *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 131–150.

[60] H. S. Sveen, F. Østrem, J. Radianti, and B. E. Munkvold, "The ciso role: a mediator between cybersecurity and top management," in *Norsk IKT-konferanse for forskning og utdanning*, no. 2. Bergen: NIKT, 2022.

[61] U. Kuckartz, *Qualitative inhaltsanalyse (German)*. Weinheim: Beltz Juventa, 2012.

[62] V. Clarke, V. Braun, and N. Hayfield, "Thematic analysis," *Qualitative psychology: A practical guide to research methods*, vol. 222, no. 2015, p. 248, 2015.

[63] V. Braun and V. Clarke, "One size fits all? what counts as quality practice in (reflexive) thematic analysis?" *Qualitative research in psychology*, vol. 18, no. 3, pp. 328–352, 2021.

[64] U.S. Department of Homeland Security, "The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research," Aug. 2012.

[65] N. Huaman, B. von Skarczinski, C. Stransky, D. Wermke, Y. Acar, A. Dreißigacker, and S. Fahl, "A Large-Scale interview study on information security in and attacks against small and medium-sized enterprises," in *30th USENIX Security Symposium (USENIX Security 21)*. Berkely: USENIX Association, Aug. 2021, pp. 1235–1252.

[66] Flynn Wolf, Adam J. Aviv, and Ravi Kuber, "Security Obstacles and Motivations for Small Businesses from a CISO's Perspective," in *30th USENIX Security Symposium (USENIX Security 21)*. Berkely: USENIX Association, 2021, pp. 1199–1216.

[67] P. Monzelo and S. Nunes, "The Role of the Chief Information Security Officer (CISO) in Organizations," 2019.

[68] A. Ford, A. Al-Nemrat, S. Ali Ghorashi, and J. Davidson, "Impact of CISO Appointment Announcements on the Market Value of Firms," *International Conference on Cyber Warfare and Security*, vol. 17, no. 1, pp. 375–384, 2022.

[69] K. E. Pearlson, C. S. Saunders, and D. F. Galletta, "Managing and using information systems: A strategic approach," 2016.

[70] I. Flechais, C. Mascolo, and M. A. Sasse, "Integrating security and usability into the requirements and design process," *International Journal of Electronic Security and Digital Forensics*, vol. 1, no. 1, pp. 12–26, 2007.

[71] S. Kamyshanskaya, "Ai and data privacy: Managing risk in the boardroom," *Board Leadership*, vol. 2021, no. 174, pp. 6–7, 2021.

[72] R. W. Masulis and S. Mobbs, "Independent director incentives: Where do talented directors spend their limited time and energy?" *Journal of financial economics*, vol. 111, no. 2, pp. 406–429, 2014.

[73] A. M. M. Al-Sartawi, "Information technology governance and cybersecurity at the board level," *International Journal of Critical Infrastructures*, vol. 16, no. 2, pp. 150–161, 2020.

[74] M. S. Islam and T. Stafford, "Information technology (it) integration and cybersecurity/security: the security savviness of board of directors," 2017.

[75] N. Vandezande, "Cybersecurity in the eu: How the nis2-directive stacks up against its predecessor," *Computer Law & Security Review*, vol. 52, p. 105890, 2024.

[76] L. Gao, T. G. Calderon, and F. Tang, "Public companies' cybersecurity risk disclosures," *International Journal of Accounting Information Systems*, vol. 38, p. 100468, 2020.

[77] S. Schmitz-Berndt and S. Schiffner, "Don't tell them now (or at all)– responsible disclosure of security incidents under nis directive and gdpr," *International Review of Law, Computers & Technology*, vol. 35, no. 2, pp. 101–115, 2021.

[78] R. Anderson, "Why information security is hard – an economic perspective," in *Seventeenth Annual Computer Security Applications Conference*, IEEE. New York: IEEE, 2001, pp. 358–365.

[79] S. Sandberg, "Lean in-women, work and the will to lead," 2015.

[80] R. Seiersen, *The Metrics Manifesto: Confronting Security with Data*. Newark: John Wiley & Sons Incorporated, 2022.

[81] L. Hayden, *IT security metrics: A practical framework for measuring security & protecting data*. New York, NY: McGraw Hill, 2010.

[82] M. Pendleton, R. Garcia-Lebron, J.-H. Cho, and S. Xu, "A survey on systems security metrics," *ACM Comput. Surv.*, vol. 49, no. 4, dec 2016.

Appendix

Interview Guides

A. Non-executive Directors

a) Unit of Analysis: The Board:

1) About yourself: (I) How many boards are you/ have you been on? (II) What is your cybersecurity (incident) experience (e.g., have you ever been on a board when a company had a major problem? (III) Have you actively educated yourself about cyber risks?
2) Board Composition: How diverse is the board? [Gender, age, educational background, experience] How diverse should it be? Who is the chairman?
3) Dynamic Responsibility: who is responsible for cyber risk at the board level?
4) Do you ever discuss cyber security with other NEDs (not in front of other board members)?
5) Are you aware of the cybersecurity policies in the company?

b) Unit of Analysis: Board Decision-making:

1) What are the key cyber risks that affect the company?
2) How is the board treating cyber risks compared to other risks?
3) How do board decisions about investment in managing cyber risks compare to other investment decisions?
4) What terms do they use to describe cyber risks?
5) How structured/controlled is the discussion on cyber risk?
6) How much time are they spending on discussing cyber risks vs other risks?
7) How much material are you given in advance of board meetings on cyber vs other risks?
8) How helpful is that material given to you in making decisions about cyber risk? Are there any problems with the material you are provided?
9) Is there other material that you would find helpful that is not provided to you?
10) Are impacts of cyber security on business considered? How?

11) Has cyber insurance been discussed at the board level?
12) Transparency: where does the board get information about cyber risks and risk management?
13) How do you assess solutions for managing cyber risk(s)?
14) What stops boards from taking the 'best' cyber security decisions (technical, investment, regulation, impact on business or staff)?

*c) **Unit of Analysis: Following up Decisions**:*

1) Are decisions about managing cyber risks being followed up?
2) Are any metrics used to assess effectiveness for managing the cyber risk?
3) Is there any discussion of the impact on the business – cost vs. benefit side effects?

B. Executive

*a) **Unit of Analysis: The Board**:* The same questions as in subsection A.

*b) **Unit of Analysis: Board Decision-making**:*

1) What are the key cyber risks that affect the company?
2) How do you see investment in managing cyber risks, compared to other investment decisions?
3) How do NEDs see investment in managing cyber risks, compared to other investment decisions?
4) How have NEDs informed the treatment of cyber risks compared to other risks?
5) What terms do NEDs use to describe cyber risks?
6) How structured/controlled is the discussion on cyber risk?
7-12) Questions 6-11 of the NEDs' b) Unit of Analysis: Board Decision-Making (see subsection A)
13) Transparency: where do you get information about cyber risks and risk management?
14) How do you assess solutions for managing cyber risk(s)?
15) Is there anything which stops your board from taking the 'best' cyber security decisions?

*c) **Unit of Analysis: Following up Decisions**:* The same questions as in subsection A, with the addition of:

1) Have you ever received complaints about the way the company manages cyber security decisions?
2) Do you ever speak to employees directly about cyber security? What do they think of the company's cyber security?

C. Chief Information Security Officer (CISO)

*a) **Unit of Analysis: The Board**:*

1) What aspects of Cyber/ Information Security are within your responsibilities?
2) Who do you report/ are accountable to? Is that person a board member?
3) Do you interact with other board members?
4) Do you think the board has the necessary expertise to make decisions on cybersecurity issues? If not, what expertise is missing?
5) How often do you interact with the board?
6) Do you think the company would make better decisions if you were a board member?

*b) **Unit of Analysis: Board Decision-making**:*

1) What information do you prepare for boards? How structured is it? Does it include any metrics/comparisons? If yes, how useful are they?
2) How much time does the board spend on dealing with the information you provided?
3) Do you get the investment you asked for?
4) What decisions do risk and audit committees make about cyber security? Are you present?
5) What is your view of cyber insurance? Would you be involved in discussions/decisions?

*c) **Unit of Analysis: Following up Decisions**:*

1) How do you implement board decisions about cyber security?
2) Who do you report back/account for the decisions you have made?
3) What do you report? Any metrics/numbers? How useful are they?
4) How do you communicate/explain cyber security decisions to employees?
5) What are the channels for reporting problems with following cyber security rules to you?

D. Members of audit/risk committees

*a) **Unit of Analysis: The Board**:*

1) What is the composition of A&R committees – who sits on the committees?
2) Who chairs it?
3) Are there any board members involved? What is their role?
4) What is decided by A&R committees, and what at board level?
5) What do you report to the board, and in what format? Any metrics/numbers? How useful are they?

*b) **Unit of Analysis: Board Decision-making**:*

1) Who sets the goals for audit and risk committees?
2) What legislation or regulation guides the work of A&R committee?
3) How do audit and risk committees implement board decisions?
4) What numbers/metrics are being used in decision-making – and how useful are they?
5) What is the interaction with the CISO?
6) What is your view of cyber insurance?

*c) **Unit of Analysis: Following up Decisions**:*

1) Who monitors progress on cyber risks? Are metrics/numbers used? How useful are they?
2) How do you decide if progress is sufficient or not?
3) Under which circumstances would you escalate a cyber security problem to board level?

Codebook

TABLE II. Our final codebook (1/2).

Code	Description	Example Quote
Relationships	Codes that describe the relationship between party A and B. This code includes descriptions of communication and direct expressions of A's and B's opinions of each other. All subcodes had the same description.	—
CISO	The view of a CISO on something; A comment of a CISO regarding something; Comments about a CISO by others	—
Internal Security Training for Management	Which kind of topics do CISOs inform the management (Board and Executives) about?	"We did something called the Cyber Series, which was basically the Audit Committee Chairman said to me, 'Can you write me a book on cyber?'" – *[CISO2].*
Security Tasks of CISOs	Security tasks and responsibilities of CISOs.	"what I do is I prepare the material for the CFO to present to the board." – *[CISO1].*
Executive	The view of an Executive on something; A comment of an Executive regarding something; Comments about a Executive by others	—
Knowledge/Awareness/Training	Direct description of an executive having (no) security knowledge, training, awareness.	"I do not think that the majority, in fact I know the majority of organizations do not take this seriously enough, and still think that it is the IT guy's/girl's job to fix this thing." – *[EX3].*
Security Information Provided	Security relevant information provided (that might be necessary for decision-making), including wishes or needs for information of an executive. e.g. reports, communicated metrics.	"For me knowing who we are dealing with is a critical capability of the firm not just from, you know, sort of, a threat actor [or] from the point of view of some cyber compromise but those that are looking to defraud or to commit other financial crimes." – *[EX4].*
Security decision-making of Executives	Security-related decision executives make or would like to be able to make.	"We consequently would have action plans of how we address certain things." – *[EX1].*
Security Tasks of Executives	Security tasks and responsibilities of executives.	"I think it works really well because he understands and he manages to put that in the bigger perspective and translate that, removing the IT, geeky world and concept out of it" – *[CISO1].*
Attitude/Opinion towards Security	Attitude: The direct expression of an opinion about the importance of security. That means some keywords need to be present, e.g., "X was very IMPORTANT to our security strategy."	"There is nothing like, you know, a real live cyber incident to prompt a change and use that burning platform to prompt a change in the organization." – *[EX1].*
The Board	The view of a board member on something; A comment of a board member regarding something; Comments about a board member, or the board in general, by others. If the executive is not talking from the board perspective, code as an executive!	—
Knowledge/Awareness/Training	Direct description of a board member having (no) security knowledge, training, awareness.	"I mean if you go to the Board and you do not really understand IT security, you do not want to spend time, or you do not have the time to understand exactly what we are doing[...]." – *[CIOS1].*
Risk and Audit Committee	Everything about the tasks, composition, responsibility of risk, and audit committee. So basically, use this code whenever such a committee is explicitly mentioned.	"Sometimes risk and audit committees take security and sometimes it's separated." – *[NED4].*
Board composition	Every statement that explains who is (not) on the board (only when related to security).	"I think there is a big theme here around Board diversity and making sure that you have people on Boards who know what questions to ask, and probably, more importantly, who understand where accountability for this lies." – *[EX3].*
Security Information Provided	Security relevant information provided (that might be necessary for decision-making), including wishes or needs for information of a board. e.g. reports, communicated metrics.	"I would like to know how we compare with other people and I would also like to know how we fit on an absolute scale if there is one." – *[NED1].*
Security decision-making of the Board	Security-related decision a board makes or would like to be able to make.	"I think most things start with the threat assessment, and then you worry about how to counter it." – *[NED2].*
Security Tasks of the Board	Security tasks and responsibilities of the Board.	"Some of the boards who have not done so well is where they have got very fixed views about how to spend the money and they are not able to adapt to changing environments." – *[CON2].*
Wishes	What do NEDs wish for?	"I would like to know how we compare with other people and I would also like to know how we fit on an absolute scale if there is one." – *[NED1].*

TABLE III. Our final codebook (2/2).

Code	Description	Example Quote
External Forces	The view of an External Force (e.g. Consultant, Regulator,...) on something; A comment of an External Force regarding something; Requirements from External Sources/Forces, e.g., Norms and Regulations; Comments about External Forces by others	—
Investors	Investors of the participant's company	"I sit through quarterly investor presentations, and I have never heard a question about it. Which is surprising, now you mention it." – *[NED2].*
Regulation	Regulatory bodies, norms, and regulations	"If you have a regulator and a regulator is asking you to prove that you have done things is also very important." – *[NED1].*
Auditing	Auditors (e.g., penetration testers) that test the security or the compliance with a norm in the organization.	"The second aspect is that you know, from a defense mechanism and ensuring that there is, for example, penetration testing that happens from a third party regularly to make sure that you're up and running, doesn't happen again in as much or as strong a manner as it should happen[...]" – *[EX6].*
Benchmarking	Comparison between different organizations.	"[...] one of the bigger influencers on the Board members is what they see, you know, if they sit on four or five Boards. You aggregate that and you get a really good perspective of how Board reporting should be on cyber." – *[CISO2].*
Cyber Risk	Every mention of some cyber risk, cyber risk assessment, or cyber risk management	—
Risk Management	How are cyber risks handled and managed? Are existing non-cyber risk frameworks used?	"I predominantly sit in financial services, so the world of finance has long had a concept of risk and risk management principles and processes and a framework. So in that sense there is an understanding of risk and there is an understanding of a process." – *[NED3].*
Risk assessment	How are risks being assessed?	"When I went to the group risk people and asked them what was the basis of their assessments of risks, it was pretty much entirely the risk of regulatory infraction because it is a highly regulated environment." – *[CON3].*
Risk Appetite	How much risk is the participant's company willing to take? How is the risk appetite set?	"The tricky one is if nothing has happened when you have not met your metrics, then the Board might be inclined to think that it doesn't matter and they could give it less money, and that might even be true, the risk appetite might be set too high." – *[NED4].*
Common Language	Risk is being described as a *common (business) language*.	"We always try and position it in the language of risk because that is the language that they understand from a board perspective." – *[CISO3].*
Company	Company specific things like reporting structures or budgeting decisions	—
Security Incidents	Any mention of an incident/attack on the own organization or on any organization if important for the attitude of the own organization.	"[company name], which had the big cyber attack that disabled their entire global operations for about ten days." – *[NED2].*
Reporting Structure	What does the security reporting structure look like?	"We used to have a federated model [...] where, for example, the Cyber Team in [European Country] only had a dotted line to me and not a hard line, and we made the flip two years ago to move all of the cyber resources in Europe into my team to create like a vertical." – *[CISO2].*
Security Budget/Investment	Any budgeting of security, any investment decision taken (or not taken).	"So for me, investment in technology biggest, biggest, biggest issue." – *[EX6].*