OPEN ACCESS JOURNALS
Indiana Journal of Economics and Business Management
Abbreviated Tittle- Ind J Econ Bus Manag
ISSN *(Online)*- 2583-3758
Journal Homepage Link- https://indianapublications.com/journal/IJEBM
DOI: https://doi.org/10.5281/zenodo.19916991

INDIANA PUBLICATIONS
PRODUCTIVE AND QUALITY RESEARCH

Research Article

Volume-06|Issue02|2026

Cybersecurity Governance at the Board Level: Challenges, Drivers and Future Directions

Nonye Peter Awurum

Charisma University, USA and British Training Center, UAE

Article History
Received: 20.03.2026
Accepted: 25.04.2026
Published: 30.04.2026

Citation
Awurum, N. P. (2026). Cybersecurity Governance at the Board Level: Challenges, Drivers and Future Directions. *Indiana Journal of Economics and Business Management, 6*(2), 46-62.

Abstract: The oversight of cyber risk management in modern organizations is a core responsibility of Boards of Directors. However, evidence indicates that board-level engagement with cybersecurity remains comparatively limited relative to other governance domains. Drawing on neo-institutional theory, this study examines the key drivers and principal barriers influencing directors' engagement in cybersecurity oversight.

Data were collected through 18 semi-structured interviews with non-executive directors across 43 organizations, providing insights into prevailing cybersecurity practices and the factors shaping board involvement. The findings indicate that regulatory requirements represent the most significant driver of engagement, reflecting strong coercive pressures. Nonetheless, many directors exhibit limited awareness of their specific responsibilities and potential liabilities in relation to cybersecurity governance.

The study further demonstrates that directors' personal experience and professional background significantly influence their level of engagement, highlighting the role of normative forces. A recurring issue identified is the over-reliance on a single board member with cybersecurity expertise. Additionally, the inherent confidentiality associated with cybersecurity constrains opportunities for inter-organizational learning and the diffusion of best practices, thereby weakening mimetic pressures.

The analysis also reveals that multiple board memberships and the involvement of external consultants exert only a marginal influence on engagement. In contrast, media coverage of cyber incidents and the prevalence of "push reporting" mechanisms emerge as more prominent organizational drivers.

Based on these findings, this study offers a set of evidence-based recommendations aimed at strengthening board-level engagement in cybersecurity governance, including the enhancement of regulatory frameworks and the standardization of cybersecurity reporting practices.

Keywords: Board of directors, corporate governance, cyber risk management, cybersecurity governance, neo-institutional theory, regulatory compliance, risk oversight.

INTRODUCTION

Boards of Directors (BoDs) oversee the complex corporate governance system of every organization. Their primary responsibility is to ensure the prosperity of shareholders and, more broadly, of stakeholders. They are accountable for regulatory compliance and the oversight of financial performance and Enterprise Risk Management (ERM). Among the latter, cybersecurity risk management (from now, cyber-risk management) is rapidly escalating the agenda of organizational priorities.

Arguably, there has never been a more important time for BoDs to consider cybersecurity as an integrative part of ERM. The ever-increasing number of cyber-breaches affecting organizations is a constant refrain that, despite the multiplication of protective measures, does not show signs of slowing down (Tsen *et al.*, 2022). Compelling evidence demonstrates how successful cyber-breaches translate into unexpected negative shocks to a firm's reputation, adversely affecting stock market activity (Tosun, 2021) and hampering the wealth of shareholders and stakeholders.

In response, BoDs have been called upon to take a more central role in governing how their companies manage the confidentiality, integrity, and availability of data and information, as this has become a vital risk for organizations (Scully, 2014; Von Solms & Von Solms, 2018; Von Solms & Von Solms, 2006).

The role of the BoD in cyber-risk management is expected to be strategic. The BoD should engage in the development of a strategic cybersecurity plan and the roadmap of its implementation rather than in its operational execution. However, several factors make strategic decision-making and oversight of cybersecurity more an art than a science, often insurmountable for non-experts (Redseal, 2016).

These factors include the intrinsic hyper-technical nature of cybersecurity (Rothrock *et al.*, 2018); the lack of directors' skills in and knowledge of this topic

***Corresponding Author:** Nonye Peter Awurum

(Aguilar, 2014; Valentine & Stewart, 2013); existing governance structures, which tend to confine cybersecurity to the kingdom of IT departments (for example, CIOs rarely report to CEOs, and most CIOs are not board members) (Grobman & Cerra, 2016); and a lack of metrics to assess cybersecurity investments.

Regulations do not seem to help. Governance standards on how BoDs should address cybersecurity oversight are still in a developmental phase and are not mandatory (ASX Corporate Governance Council, 2019; Federation of European Risk Management Associations, 2018).

Researchers have often described the boardroom as an impenetrable black box (Watson *et al.*, 2020). It is thus unsurprising that, besides prescriptive industry publications and descriptive statistics (Enterprise Strategy Group, 2020; PwC, 2021), it is still unclear how BoDs currently address and understand cyber-risks.

Existing literature on the role of organizational leaders in cybersecurity management focuses on limited topics, predominantly on the management of information systems. Examples include how audit committees address cyber-risks and oversight (Lankton *et al.*, 2021); how top managers' perceptions shape organizational commitment to cybersecurity strategy (Ogbanufe *et al.*, 2021); how senior leaders affect employees' compliance with information security policies (Hu *et al.*, 2012); and generic guidance and recommendations for managing cybersecurity (Renaud *et al.*, 2019; Zukis, 2016).

The scarcity of research calls for an in-depth, exploratory study to generate "insights about corporate governance practices" (Zattoni *et al.*, 2013, p. 121) regarding cybersecurity. In this domain, both academic and practitioner literature acknowledge the existence of a gap between top leadership and IT departments (Schinagl & Paans, 2017; Tripwire, 2019).

Practitioner literature mainly entails "how-to" guides and recommendations for directors when they discuss cybersecurity with IT specialists and other executives (Cohn *et al.*, 2017; Renaud *et al.*, 2019; Rothrock *et al.*, 2018). What remains unclear is whether and how such recommendations translate into boardroom activity. To the best available knowledge, no prior study has explored this uptake and its effectiveness. This is the gap the present research intends to address.

This research investigates directors' engagement in cybersecurity by adopting the rigorous lens of neo-institutional theory to analyse the dynamics that characterize directors' discussions and decisions in this field (AlKalbani *et al.*, 2017; Ogbanufe *et al.*, 2021).

The theory predicts that, in the face of high uncertainty and to gain legitimization, organizations (in our case, BoDs) imitate practices of comparable organizations (DiMaggio and Powell, 1983). Coercive (e.g., regulations), normative (e.g., professionalization, education and training, experience, diffused expectations about specific behaviors), and mimetic pressures (e.g., diffusion of imitative practices through, for example, circulation of professionals and external consultants) drive this phenomenon, called institutional isomorphism.

However, the three types of pressures do not act in a vacuum. Surrounding organizational factors also play a significant role (Jeyaraj & Zadeh, 2020).

This study addresses the following two research questions:

- How do directors currently engage in cybersecurity?
- Which factors drive directors' engagement in cybersecurity?

The following section illustrates the methods adopted in our research. Subsequently, we discuss our findings. We then offer a discussion of our results, followed by concluding remarks.

LITERATURE REVIEW

The Engagement of Board of Directors in Cyber Risk Management

Generally speaking, within the discipline of risk management, the directors' role is one of oversight (Leblanc & Fraser, 2016). How proactively such oversight should be exercised in cybersecurity is a matter of considerable contention. In theory, senior management and directors determine their organisation's risk profile and strategy. Senior managers regularly report to BoDs and update them on the organisational performance to help them perform their oversight function (Landefeld *et al.*, 2015).

However, in cybersecurity, the theory appears in contrast with current practice. A study by the Ponemon Institute found that 60% of surveyed IT employees fail to report cyber-breaches to their BoDs unless they are "serious" and otherwise tend to omit overly negative results from reports (Martin, 2014). Furthermore, another recent report by Enterprise Strategy Group (2020) revealed that, out of the 365 senior professionals surveyed, 69% perceive that cybersecurity is primarily still a technical domain, and 85% indicate that BoDs are becoming more involved in cybersecurity matters, but still have considerable room for improvement in carrying out their duties.

A powerful synthesis has been provided by US Securities and Exchange Commissioner Luis A. Aguilar, who remarked in 2014: "...evidence suggests that there may be a gap […] between the magnitude of the exposure presented by cyber-risks and the steps, or lack thereof, that many corporate boards have taken to address these risks…" (Aguilar, 2014, p. n.d.).

At the same time, several concurring dynamics are steering BoDs toward a more active and effective practice of cybersecurity governance (Scully, 2014). The first of these is the growth of destructive cyber-breaches, with ransomware attacks being the latest booming trend (Tsen *et al.*, 2022). Multiplication of notable cases of major cybersecurity accidents has elevated cyber events to potentially life-threatening for many affected organizations (Center for Strategic and International Studies - CSIS, 2021).

Second, a seemingly unrelenting increase in cybersecurity spending by companies worldwide requires boards to approve ever-larger budgets for cybersecurity. Advisory firm Gartner predicts global cybersecurity spending will exceed $150 billion by the end of 2021, which represents a 12.4% growth from 2020 (2021).

Third, mounting regulatory pressures[1] are compelling larger and highly regulated organizations to intensify their defensive efforts or run the risk of incurring hefty fines. This trend also urges top organizational leaders to react.

The resulting uplifting of cybersecurity "from the basement to the boardroom" (Schinagl & Shahim, 2020) has recently been a process conceptualized on paper but ill-defined in practice. Recent research shows that in Australia only 3% of directors have a background in STEM disciplines (Australian Institute of Company Directors, 2020). Organizational leaders that do not possess a background in cybersecurity, are not aware of regulations or are not familiar with emerging threats, industry trends, and existing benchmarks, and therefore struggle to exercise their duty (EY & Institute of Internal Auditors, 2021; Mishra, 2015).

Despite a wealth of frameworks, standards, and guidelines (e.g., NIST Cybersecurity Framework, NIST Special Publication 800-53, ISO Standards 27001/2/5, COBIT19 (Leszczyna, 2018)) available to inform cyber-risk management in modern organizations, guidance on the role of BoDs is, at best, scarce.

Existing cyber-governance models do not seem to help either. The proposed transition from the Three Lines of Defense model for cybersecurity (operations, risk management and compliance, and internal audit) to the Five Lines of Assurance model has conceptualized an enhanced role for BoDs in cybersecurity governance; however, without offering practical strategies for implementation (Leech & Hanlon, 2016). The suggestion that a risk-based approach to cybersecurity (as opposed to a maturity-based one) would allow BoDs to adopt precise targets to reduce cyber-risks (Boehm *et al.*, 2019) does not provide practical solutions.

Additionally, individual factors further complexify proactive oversight by BoDs in cybersecurity. Hartmann and Carmenate (2021) emphasise that BoDs still have dated views about cybersecurity. A study on the IT confidence gap revealed that most directors are in their sixties, educated before the digital age, and tend to be overwhelmed by technical jargon (National Association of Corporate Directors & Internet Security Alliance, 2020).

Descriptive statistics support these findings. According to a recent survey by PwC (2021), only 53% of US directors "somewhat understand" cybersecurity. Interestingly, current trends seem to point towards a decrease in directors' confidence in cybersecurity reports. Australian law firm Minter Ellison reported that in 2020 a declining number (20% compared to 35% in 2019) of their respondents (organisational leaders in cybersecurity and risk management) have a "very good understanding of their organisation's exposure to the risk of cyber-attacks" (Minter Ellison, 2020).

In response to the lack of technical knowledge in the boardroom, specific committees that advise BoDs on technical matters have been created (Landefeld *et al.*, 2015). Research suggests that the effectiveness of committees in fulfilling their purpose increases with their members' competencies (Bajra & Čadež, 2018). With committees being a subset of BoDs, the quality of cybersecurity decisions made by the boardroom is only as great as the knowledge of its committee. However, the fiduciary responsibility for cybersecurity ultimately rests with the BoD, not the committee. Therefore, whether or not the BoD deems cybersecurity as a strategic matter is perceived through the lens of their collective experiences, education, and background (Hartmann & Carmenate, 2021).

This literature review demonstrates that the issue of whether BoDs should oversee cybersecurity is no longer debatable. Given all the difficulties faced by BoDs, the essential question that needs to be addressed is: "How should BoDs more proactively engage with cybersecurity?" To answer this, we first need to better understand current practices on cybersecurity engagement in the boardroom. To the best of our knowledge, in-depth evidence on this currently does not exist (Watson *et al.*, 2020). We aim to address this gap, before offering practical recommendations for BoDs to govern cybersecurity more effectively. Next, we illustrate our theoretical framework, anchored in neo-institutional theory.

Conceptual Framework: Neo-Institutional Theory and Its Application to Cybersecurity

It has been demonstrated that current attitudes, practices, and perceptions by directors vis-à-vis cybersecurity are influenced by a complex mix of regulatory pressures, individual predispositions and background, preliminary knowledge of the topic, pre-existing governance structures, and industry best practices.

Neo-institutional theory (DiMaggio & Powell, 1983) provides an account for all of the above in a framework that, besides offering a taxonomy, provides support in identifying practical recommendations for BoDs. According to neo-institutional theory, specific institutional pressures influence the way in which organisations make decisions in a variety of fields (DiMaggio & Powell, 1983).

The theory suggests that organisational practices are driven by the need for legitimacy more than the need for efficiency and effectiveness. This results in organisations adhering to similar institutional norms, converging towards a set of comparable structures, processes, and designs (called institutional isomorphism) (Lawrence & Shadnam, 2008). Three main pressures push organisations towards isomorphism: coercive, normative, and mimetic (DiMaggio & Powell, 1983).

Despite its tradition in other fields, neo-institutional theory has only recently been applied to cybersecurity (AlKalbani *et al.*, 2017; Haislip *et al.*, 2017; Jeyaraj & Zadeh, 2020; Kabanda *et al.*, 2018; Ogbanufe *et al.*, 2021; Vuko *et al.*, 2021), and never to the role of BoDs in cybersecurity oversight. We now illustrate the three types of pressures through the lens of prior work in cybersecurity and reflect on how these pressures can affect directors' roles.

Coercive pressures are characterised by regulations (e.g., CCPA, GDPR, or NDB Scheme) and industry standards (e.g., Payment Card Industry Data Security Standards – PCI DSS). Information privacy laws and regulations sanction non-compliance with significant fines. As a result, organisations bound by them adopt similar rules, practices, and governance mechanisms in a relatively short time (Jeyaraj & Zadeh, 2020). Although regulatory compliance is seen only as a minimum and not as an effective cyber-risk management strategy (Vuko *et al.*, 2021), it can have a significant influence on directors' behaviours (AlKalbani *et al.*, 2017). Many of them see ensuring regulatory compliance as one of their main duties. Personal motives are important too, as a director's role entails personal liability. Depending on the jurisdiction, some constituencies believe that the directors' duties in cybersecurity are currently well captured under existing company laws and/or federal/national regulations. For example, the Australian Corporations Act 2001 (Cth) already defines the directors' obligations of care and diligence and of acting in good faith and the company's best interests. These obligations also extend to cybersecurity oversight. Others believe that current regulations do not offer a clear-cut answer regarding directors' personal liability vis-à-vis cybersecurity oversight. The discussion paper "Strengthening Australia's cyber security regulations and incentives" (Australian Government, 2021) calls for a strengthening of regulations in the field and for developing future governance standards for BoDs to ensure that cybersecurity is more adequately addressed.

To date, there have not been many successful lawsuits against BoDs following cyber-breaches (Lacroix, 2016), which lends support to the latter viewpoint. However, several lawsuits are currently ongoing (Cyber Security Cooperative Research Centre, 2021) and the outcomes remain to be seen. Certain industry-specific regulations, most notably financial prudential regulation, better define directors' liability in cybersecurity oversight (e.g., the Prudential Standard CPS 234 Information Security (Australian Prudential Regulation Authority, 2019); the European Banking Authority Guidelines on ICT and security risk management (European Banking Authority, 2019).

Normative pressures are determined by professionalisation, which defines specific work methods and practices associated with a profession (DiMaggio & Powell, 1983). These pressures develop through formal education and training, professional certifications, direct and mediated experience, and adhesion to professional standards and networks (Vuko *et al.*, 2021). Normative pressures manifest, for example, through certifications often required from cybersecurity professionals (Columbus, 2020). With these certifications, professionals tend to promote structures, processes, and behaviours recognised as good practice in cybersecurity. Another example of normative pressures in cybersecurity is the role played by the media. The media shapes expectations around virtuous behaviours in cybersecurity (e.g., by pushing organisations to protect customers' data). In general, normative pressures tend to manifest over a long-term period (Jeyaraj & Zadeh, 2020). The extent to which directors rely on certified cybersecurity professionals and the extent to which normative pressures affect directors in their cybersecurity oversight still remains to be understood.

Mimetic pressures are mostly at play in situations of high uncertainty. Organisations that are perceived as particularly legitimate serve as role models that other organisations mimic to legitimise their practices. In this sense, information sharing about practices, actions, and behaviours is particularly important. In cybersecurity, the circulation of professionals across organisations, hiring the same external consultants, purchasing technology from the same vendors, and consulting the same publications, are all mimetic forces. These forces tend to have long-standing effects in influencing cybersecurity decisions (Jeyaraj & Zadeh, 2020). As for the directors' role, mimetic pressures can manifest when directors sit on BoDs of multiple organisations and transfer board practices across organisations. Taking on cyber-insurance, for example, can be a result of directors sharing positive views on it.

Despite their significant influence on organisational decisions, institutional pressures are not exerted in a vacuum. Research shows the importance of circumstantial, organisational factors. Kabanda, Tanner, and Kent (2018) found that SMEs in developing countries are significantly constrained by a lack of managerial and BoDs' support and consequent budgetary limitations in their quest for cybersecurity. Vuko, Slapničar, Čular, and Drašček (2021) recently demonstrated that the support and competency of BoDs are fundamental drivers of an effective cybersecurity audit. Together, organisational factors can outperform the effect of coercive ones. Lastly, organisations affected by past cyber-breaches may be more proactive in responding to additional cyber-attacks (Jeyaraj & Zadeh, 2020).

The literature review has highlighted that organisational factors interact with institutional pressures to drive the diffusion of effective cybersecurity practices (Damenu & Beaumont, 2017; Ogbanufe *et al.*, 2021; Renaud *et al.*, 2019; Schinagl & Shahim, 2020; Zukis, 2016). Yet, the knowledge about how this applies to BoDs' engagement with cybersecurity is largely incomplete. Figure 1 illustrates the conceptual framework adopted in the present research and how it allows us to address our two Research Questions.

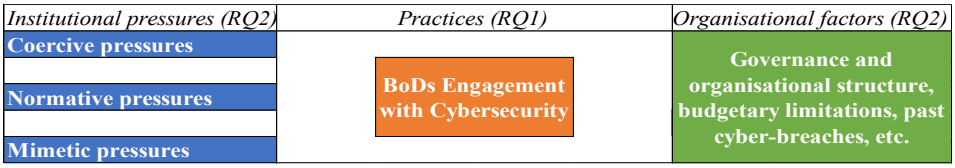

Figure 1: Conceptual Framework of Institutional and Organizational Factors

Note: RQ1: How directors currently engage in cybersecurity? and RQ2: Which factors (institutional pressures and organisational factors) drive directors' engagement in cybersecurity?

RESEARCH METHODS

Overview

The present study stems from an interpretivist paradigm and the endeavour to make sense of the human experience (Lincoln *et al.*, 2011). The previous literature review demonstrated that our understanding of directors' engagement with cybersecurity is largely incomplete. As a result, we adopted an exploratory perspective (Babbie, 2013) and a qualitative approach, which is reputed as the most appropriate for inductively gathering and analysing data (Billups, 2020).

To promote a deep, meaningful understanding of cybersecurity discussions in the boardroom by exploring the narratives, views, and experiences of directors who hold responsibility for cybersecurity governance, we conducted 18 in-depth, semi-structured interviews with Non-Executive Directors (NEDs) representing 43 Australian organisations across diverse industries.

To achieve its purposes and address the two RQs, this study followed Stake's (1995) guidance for a flexible research design, acknowledging that the issues and perceptions raised by participants could not be known at the outset, consistent with an inductive modus operandi.

Sample

We adopted a purposeful sampling strategy (Patton, 2015) to identify participants who had experience with the subject matter as NEDs in Australian boardrooms, from public and private companies (including special purpose government entities) and incorporated associations. Both the current regulatory framework (Australian Government, 2001) and the proposed one (Australian Government, 2021) make these NEDs "information-rich" participants for the purposes of this study (Patton, 2015, p. 53).

The richness of the collected data was significantly magnified by the fact that most NEDs in the sample held more than one directorship position, expanding the sample size of organisations to 43 (Table 1).

Table 1: Number of participants' directorships

Header	None of One	Two	Three	Four	Five
Number of current directorships	4	6	6	1	1

Table 2: Industries represented in the sample

Industry	#
Financial Services	8
Healthcare	6
Retail	1
Sport	3
Aged care	2
Local Government	2
Education	5
Media and Arts	2
Professional services	6
Employment services	1
Community services	4
Technology	2
Utilities/Infrastructure	1
Total organisations	43

***Corresponding Author:** Nonye Peter Awurum

Table 3: Organizational Types

Category	Type
Proprietary company 11	11
Public (unlisted) company 9	9
Public company/Not-for-profit 9	9
Incorporated/Registered	5
Government/Special purpose 6	6
Australian Stock Exchange Listed 1	1
Partnership 2	2
Total	43

Data collection and analysis

Several strategies were adopted to recruit participants such as introduction through an organisation dedicated to training directors and facilitating networking; contact through social media platforms (e.g., LinkedIn); and snowballing (Marshall & Rossman, 2011), when a participant introduced the research project to other NEDs.

We obtained ethical approval for this study from our university before data collection. We conducted semi-structured interviews in which we asked open-ended questions to elicit informational, personal, or descriptive data from the participants (Billups, 2020). Interviews followed a protocol (Appendix A), which provided standardisation whilst allowing the flexibility to follow leads and customise questions as needed. Respondents were, in fact, free to probe beyond the answers. The semi-structured flexibility favoured discovering the experiences, perceptions, and involvement of directors in cybersecurity. The protocol followed Kvale's (1996) staged approach with an emergent sequence of (1) narrative, (2) detail, and (3) participant perspective. Billups (2020) promotes this emergent approach as best for semi-structured conversations. We designed our questions as "tell me how" type of questions (Spradley, 1979). Questions advanced from general to specific (Patton, 2015), first framing the topic and then focusing more on the questions underlying the whole research project. All researchers were involved in the formulation of the interview questions and extensive discussion and adjustments preceded finalisation of the interview protocol.

Interviews ranged from 32 minutes to 1 hour 28 minutes (on average: 1 hour 5 minutes). Participant consent was sought at the start of each interview. Confidentiality and voluntary participation statements were discussed with each participant. Due to COVID-19 restrictions, interviews were conducted virtually through Zoom. Billups (2020) argues that online interviews are as effective as in-person ones (as a collection of non-verbal behavioural information is equally achievable). All interviews were recorded and transcribed by the researchers, who then reviewed the transcriptions for accuracy. We pseudonymised the transcripts to protect the anonymity of the participants and the confidentiality of data.

We analysed our data using a thematic analysis approach. In line with exploratory research, this allowed flexibility in the analysis process for a rich and detailed assessment and presentation of the findings (Marshall & Rossman, 2011). During data collection, emergent themes were identified by the researchers after each interview. These were noted and referred to after each subsequent interview to locate commonalities. Themes were descriptive at this stage (Locke, 2001), remaining close to the words of NEDs. Using Miles and Huberman's (1984) approach (pattern, descriptive, and interpretive), secondary coding and recoding followed. Finally, relationships between themes were discussed among the researchers and compared to relevant literature. This process was used to ensure collected perceptions and experiences were genuinely captured and interpreted within the boardroom context.

Research evaluation

Seminal work by Lincoln and Guba (1985) and Lincoln, Lynham, and Guba (2011) suggests that trustworthiness, and its four components credibility, dependability, confirmability, and transferability, are the criteria to evaluate qualitative research. Credibility measures the extent to which the findings highlighted by the study are congruent with the examined reality. In our investigation, we followed Patton's advice (2015) and combined rigorous methods (plus a conceptual framework anchored in the well-established neo-institutional theory) with the credibility of the researchers, and a philosophical belief in the value of qualitative inquiry, to achieve credibility. Dependability means obtaining the same results when the investigation is repeated under the same conditions by other researchers. Following Shenton's recommendations (2004), we achieved this by detailing the adopted research process to allow fellow researchers to replicate our investigation (see also Appendix A). Confirmability indicates the findings' independence from biases which might affect investigators. To achieve confirmability, we adopted three strategies (Yin, 2009). First, chains of evidence throughout our research stages were established, from data collection to elaboration of the conclusions. Second, thematic coding was independently verified by the three researchers, and results discussed until an agreement among the researchers was achieved. Third, at the end of each interview, respondents were given the possibility to expand on their answers or amend parts of them, based on a summarising conversation with the interviewer. Transferability indicates generalisability of findings to a broader population. By nature, all qualitative research has limitations in terms of transferability (Marshall & Rossman, 2011). To limit the impact of this, methodologists suggest several strategies, which we adopted in our investigation. First, our sample of 18 interviewees represents 43 organisations in Australia, a sample size within the range of studies adopting a similar interpretive approach (Marshall & Rossman, 2011; Yin, 2009). Second, we carefully itemised the adopted research methodology by providing

the readers with specific information about the research design, the data collection methods, the sampling strategy, etc. This is expected to help readers independently assess generalisability of our findings (Shenton, 2004). Third, as we conducted our final interviews, data saturation was reached and no new themes emerged from the data for our analysis (Ando *et al.*, 2014).

FINDINGS

Directors' engagement with cybersecurity

All interviewees had strong opinions about the fact that cybersecurity should be on their boardroom agenda, but how frequently that occurred was highly debatable. Generally, participants raised concerns about the level of interest in, and understanding of, cybersecurity:

> *"Cyberspace and cyber governance are at the heart of risk and boards aren't in that space." [2]*

Participants frequently described their fellow directors' shying away from discussions on cybersecurity or submitting to the views of "onlookers" to the subject. In the case of itemised cybersecurity discussions, boards were best described as silent or reluctant. When asked about the reasons for this, a third of participants characterised this as a form of personal protection: either protection of ego (due to lack of knowledge in the area) or protection from personal liability (e.g., directors relying on more knowledgeable colleagues to take responsibility for cyber-governance).

Our data also revealed that the reason for cybersecurity not being on the board's agenda, or being a low priority item, was the NEDs' lack of confidence in discussing cybersecurity. One of them, who demonstrated above-average knowledge of the topic (having completed cyber-governance training), and whose organisation's approach to cybersecurity appeared advanced, commented on their organisation's approach to cybersecurity as follows:

> "We're at a lower level of maturity, I guess, in our overall risk management, and that's inclusive *of cyber risk." [11]*

Although a third of participants initially stated that cybersecurity had not been discussed in the boardroom, they then stated that cybersecurity had been raised as an operational risk in boardroom discussions. However, these same individuals also reported that several fellow directors did not engage in those discussions. When asked for a judgment on the practice of not addressing cybersecurity in the boardroom, one participant qualified the concept as "terrifying" [IDI-8].

Half of the participants admitted that because cybersecurity mainly represents an unknown risk, it cannot be easily alleviated. Some of those participants appeared to apply this caveat to their responsibilities, or rather difficulties, in addressing cybersecurity, which was framed in somewhat fatalistic terms:

> *"It's not if, but when. So, it's less about trying to be [proactive], and more about when we do have [a cyber-attack], how are we going to recover." [18]*

Collected data revealed that the boards frequently delegate responsibility for cybersecurity to the audit and risk committees. Respondents considered the committee, not the entire board, as responsible for overseeing cybersecurity reporting (e.g., from the CEO, Chief Information Officer – CIO, or Chief Information Security Officer - CISO). The committees then report only very condensed information to the board. Cybersecurity reporting is only one component of organisational risk reporting in those reports.

Half of the participants reflected that cybersecurity is not usually an agenda item for board discussion unless there is an exceptional circumstance (such as a near miss or a cyber-attack). One participant described one such attack in 2020. The respondent [7] reflected that, prior to that incident, cybersecurity had been raised "in terms of IT expense" and "what IT is providing, actually doing, and could offer". It had been considered that the board had delegated cybersecurity to either the IT department or the CEO. Following the cyber-attack, the board added cybersecurity to its risk matrix:

> *"That's a standing agenda item for every meeting, so while we may not discuss it in detail […], it's just a standing item. When we get to the risk matrix, we just reassess all the risks, including cyber risks as well." [7].*

Another participant also explained that before their organisation suffered a cyber-attack, cybersecurity was not an agenda item for discussion but rather a tick-box action item. A cybersecurity policy would be periodically raised for review and approved without meaningful debate.

The Effect of Institutional Forces

Coercive Pressures

Besides these general findings, our data highlighted the significantly different intensity of cybersecurity discussions in the boardroom between organisations that are regulated by the financial prudential regulator (the Australian Prudential Regulation Authority - APRA) and those that are not.

As for the directors of APRA-regulated organisations, discussions on cybersecurity are more frequent, mostly on disaster recovery, regulatory auditing, and compliance with CPS 234 (Australian

Prudential Regulation Authority, 2019). In their interviews, all of these directors reported an upcoming compulsory audit by APRA on their cybersecurity management. Yet, just as the directors of non-APRA regulated organisations, these interviewees noted that discussions would be relatively high-level and initiated mainly by risk and audit committees within the board. Amongst the addressed sub-topics are cyber-insurance, penetration testing requirements, business interruption, testing data recovery systems, investments in cybersecurity, and considering whether (or in what circumstances) their organisation would pay a ransom.

Participants expressed that their organisations experience significant regulatory pressure to formulate, implement, and monitor an organisational cybersecurity strategy:

> *"As an APRA regulated ADI [Authorised Deposit-taking Institution], we have to comply with CPS 234, which is all about cyber governance ...so we spend a lot of time understanding our cyber governance and feeding that structure as part of our risk management framework." [8].*

> *"We've been working towards making ourselves compliant [with CPS 234] over that time frame [since July 2019] ... Introduced policies; one is data governance." [11]*

One participant commented on other directors in the banking industry referring to CPS 234 as "new," suggesting that cybersecurity should have been on the agenda long before its official introduction:

> *"Some of the latest Australian standards or APRA standards around cyber, you know, people say they're new. They're actually not. I saw the first draft and worked on the first draft with the regulator; I think it was in 2009." [9].*

Another participant, who sits on both APRA-regulated and non-APRA regulated boards, observed the latter to be far less sophisticated than the former in addressing cybersecurity issues.

In non-APRA regulated organisations, seven (i.e., 70% of this subset) participants reported that cybersecurity is discussed infrequently and at a high level, as a suggestion for a future conversation or as something for the "to-do list". Amongst the addressed sub-topics are organisational information systems, email infiltration, penetration testing requirements, disaster recovery, and consumer protection. Interestingly, only one respondent mentioned cyber-insurance as a matter of discussion in response to a specific cyber-threat. Among these organisations, the sole other circumstance in which cybersecurity discussions are initiated at the board level is after a successful cyber-attack or a significant cyber-threat materialising, with the board discussing how to mitigate the associated impacts. Three participants mentioned this instance.

Personal knowledge of regulations appeared to be an important factor: the majority of interviewees from non-regulated organisations were unaware of regulations or standards related to cybersecurity. A couple of participants referred to the ISO27000 series (Leszczyna, 2018) but acknowledged these are not regulations. Three respondents questioned rhetorically whether the Privacy Act 1998 (Australian Government, 1988) might apply to their organisations. Five participants asked the researcher if there were any regulations they should be aware of. Director duties were sometimes cited as a consideration, although with apparent uncertainty. By contrast, one director commented with some authority:

> *"There's not a lot of regulatory oversight in the general run of Corporations Law, other than if you're not looking at it [cybersecurity], you're not exercising due care and diligence, and you're probably not fulfilling your role as a director." [8]*

Normative pressures

A third of participants considered their personal IT or cybersecurity experience, or that of a fellow board member, as the driving force "pushing" cybersecurity into their board's agenda. Most respondents also argued that directors who are not addressing cybersecurity on their boards would be embarrassed to admit it. Despite this, most of our interviewees did not identify skills in cybersecurity as necessary for the proper functioning of their boards, their task of overseeing risk management or meeting their respective duties. On the contrary, legal, accounting, and HR skills were identified as required for these purposes. Having skills in cybersecurity by a director was described as a "point of differentiation" by one participant.

Only a few participants mentioned any hiring focus on directors with cyber-skills, and no participant was aware of any intention for their current boards to do so in the foreseeable future. Those who identified the need for cyber-skills in their board skills matrix were predominately from APRA-regulated entities.

Thirteen participants in our sample considered themselves influential in cybersecurity discussions in their boardroom despite not having any formal qualifications or training in this field. Five participants recognised another fellow board member as influential, and only if this individual has qualifications in cybersecurity or the participant believed the individual truly understands or is actively engaged in cybersecurity. One participant described the influential director as "technical, geeky." Perhaps perversely, it was this technical ability that the respondent said needed to

change for that director to be an effective contributor to their board:

> *"He loves the technical end, and he hadn't had a lot of board experience […] so part of the education process for him, and with us, has been to take himself out of the technology provider space, and you know, resist the temptation to go and do it and look more at the policy settings and the strategic approach to the risk management framework." [8]*

Overall, our data emphasised that where participants have an interest in cybersecurity, or a background loosely connected to IT, that is sufficient for fellow board members to rely on them as "responsible" for cybersecurity in the BoD. Boards let them interpret cybersecurity reporting or lead the board (and even the organisation) on, for example, achieving cyber-resilience:

> *"We've had to use our board member who's well versed in this [cybersecurity] as an interpreter from time to time." [8].*

A few respondents noted that the presence of such a director appears to implicitly minimise the duty for fellow directors to upskill in, or proactively contribute to, discussions on cybersecurity. Conversely, directors with cybersecurity experience noted the reliance that their fellow directors often place on them:

> *"I tend to try not to lead it [conversations on cyber], though, because I want others to really have some air and talk about their concerns and their viewpoints, and really get involved in those conversations." [9].*

The same participants also mentioned shying away from driving cybersecurity conversations for fear of making the discussion too technical and intimidating or for concerns over personal liability.

Interviewees from BoDs who have undertaken cybersecurity training reported more confidence in asking questions about reporting and engaging in cybersecurity discussions overall:

> *"A little bit of knowledge can be dangerous. I think we have enough knowledge to be at least asking questions from a reasonably sensible place and able to check in with ourselves whether we think the answers we're getting are sufficient." [8].*

Nonetheless, the increase in confidence brought by cybersecurity training was described as marginal, as several respondents argued that training does not alleviate reliance on reporters or fellow directors with identified cybersecurity skills.

Our data revealed that professionalisation and experience considerably affect the content of cybersecurity reporting and, consequently, the level of directors' engagement in this field. Despite being largely dependent on their reporters, as presented in more detail below, almost all participants hesitated when asked what qualifications the reporters have in cybersecurity and why they relied upon them. Four specifically mentioned different individuals in the organisation whom they considered as having expertise in cybersecurity and/or experience with cyber-breaches (e.g., working from CIO down to a specific employee within the IT team or an IT consultant):

> *"He led a core banking conversion, and he's subsequently led projects [where] we've had to do data conversion into our systems. So, he's having some great exposure…he's been involved where a couple of incidents have occurred. They weren't cyber threats, but they were incidents within the system." [11].*

Lastly, an interesting finding related to the role of media reports about eminent cyber-breaches in driving cybersecurity discussions in the boardroom. One participant described the impact of media and cyber-related news as a trigger for directors' engagement in cybersecurity discussions. Our data revealed that media articles on cyber-attacks are often shared among directors either via email or directly at board meetings. However, participants described these discussions as peripheral to the formal board agenda, more conversational, and simply "of interest" rather than actionable. More on the role of media reports is in section 4.3.

Mimetic pressures

One of the interview questions asked participants to identify best practices or industry guidelines to drive the formulation of cybersecurity strategies in their organisations. Respondents could not mention any. As for APRA-regulated entities, our data demonstrated that privately funded consulting reports provide boards with a very general understanding (e.g., on cybersecurity maturity levels) of how their organisation is performing against other APRA-regulated entities in compliance with CPS 234 (Australian Prudential Regulation Authority, 2019). Most of those reports were commissioned as an audit activity mandated by regulations.

Similarly, collected data revealed that approximately 80% of respondents did not know how, or even if, their competitors were addressing cybersecurity. For those who did, competitors' practices were drawn from reported cyber-attacks, utilised as case studies for learning purposes. Many participants referred to competitors' benchmarking as "really challenging" in cybersecurity.

Other interviewees reflected that either themselves or fellow directors have experience with cyber-attacks or significant near-misses and cyber-threats whilst serving on other boards. They would then share learnings and recommendations from these events in their other organisations.

Another source of mimetic practices emerging from our data are external management consultants. Our interviewees explained that they are not regular reporters to boards but are still a key driver for organisational configuration of, and investment in, cybersecurity. Two main factors were singled out as reasons to engage external consultants: as part of an external audit mandated by regulations (e.g., APRA); and as an internal audit initiated by a director with cybersecurity audit experience or encouraged by top management.

Organizational Factors

We also investigated the impact that organisational factors have on BoDs' engagement with cybersecurity. Our data highlighted three main factors: cybersecurity reporting practices, the effect of past cyber breaches affecting the organisation, and unrelatable media reports about eminent cyber breaches.

The data revealed four main sources of cybersecurity reporting: executives/senior management (e.g., CEO, CIO, CISO) or other senior business managers; internal or external IT teams; audit and risk committees; and external management consultants. Mostly, respondents lamented a communication gap between directors and reporters due to information asymmetry. Reporting is bottom-up, with the content of reporting being almost entirely at the discretion of the reporters. At the same time, there seems to be little understanding about what directors want to be reported on, to support their oversight role in cybersecurity. Interestingly, most respondents admitted that BoDs do not usually set clear expectations on reporting activities, yet they nevertheless expect reporters to be aware of directors' expectations:

> *"But no one's placing an expectation, and certainly [the Chair]'s not placing an expectation on any kind of reporting around some of these things…No one's set up a reporting system that expects [the head of IT] to send that information through, so there's no awareness at the board level about what really goes on. Everyone just assumes it'll be looked after by [the head of IT]." [15].*

As one participant explained, in their organisation the IT team decides what to report to the CIO. The CIO then condenses that information and decides what to report to the audit and risk committee. The audit and risk committee further summarises that information in its report to the BoD.

Fifteen participants could not mention specific key performance indicators (KPIs) against which the success of cyber-risk management is measured, leaving the impression that reporters self-regulate and assess their own effectiveness. Directors generally emerged as not challenging information contained in cybersecurity reports and its interpretation; identification of significant cyber-threats or vulnerabilities; nor information on the organisational cyber-risk profile. Trust in the reporters mainly seems to be guaranteed, based on the authority of the position (such as, for example, a Chief Technology Officer - CTO). One participant revealed that it was their CTO who once identified the need for more "plain English" cyber-reporting, including reformatting the report to be more diagrammatic (e.g., usage of "traffic lights"). This appeared to be done to encourage board members to interact more with the reporting, particularly within APRA-regulated entities.

When asked about the quality of cyber-reporting, three respondents (including those with a technical background) mentioned a lack of clarity or relevance, as witnessed by this excerpt (the respondent has cybersecurity experience):

> *"I've provided some recent feedback on that report. I don't really know what that report is telling me…. Don't get me wrong, there's really good stats in there […], but what is it telling me? What should I derive from that report? That we are operating within our risk appetite? Where's my emerging risks? […] Should it be keeping me awake at night?" [9]*

On another note, several respondents explained that reports often contain high numbers of "near misses" or "cyber-threats": and those numbers tend to be meaningless because neither the nature nor the significance of the threats are identified. This results in a diffused sense of complacency. One participant remarked that if the threats were given names, or how viruses operate was described, directors might be more engaged:

> *"I couldn't care whether there's a million spam emails a day or a million attempts to hack into the organisation. That's just hygiene these days… Tell me about the things that aren't operating effectively, tell me about the emerging things we're not sure about, where we may get compromised, and what are we doing about it." [9]*

Directors also discussed that when reporters do not direct them to consider any information in the report specifically, they subsequently feel there is no outstanding cybersecurity issue.

Cyber-attacks affecting an organisation have a perhaps expected influence in driving cybersecurity conversations at the board level:

> *"Once you have been subject to an attack […], you give it [cybersecurity] more attention. You give it more airtime at the table because it's true […] so yeah there's nothing like those sorts of things happening that shuffles up the agenda." [8]*

One participant discussed their organisation suffering an attack whereby their email system was infiltrated at various points. Upon reflection on the circumstances of the attack, the participant remarked:

> *"The organisation was blaming the IT people, and the IT were blaming the organisation." [7]*

Following the event, the board immediately added cybersecurity to its risk matrix.

Finally, our respondents also highlighted how media reports about an eminent cyber-event could cause directors to dismiss cybersecurity. They explained that this is the case when a mediatic cyber-event occurs to an organisation perceived as being larger, more important, and generally more attractive than the director's, resulting in the latter's disengagement with the topic.

DISCUSSION

How do directors currently engage in cybersecurity (RQ1)?

Confirming findings from prior quantitative studies (Australian Institute of Company Directors & Roy Morgan, 2021), our research demonstrates that, in normal circumstances, cybersecurity does not receive sufficient attention in Australian boardrooms. Several reasons explain this.

First, despite advancements in the field (Soomro *et al.*, 2016), cybersecurity is still perceived as a mainly technical issue, requiring background knowledge to be appropriately discussed (Abu-Musa, 2010). In our investigation, lay directors tend to retreat from a discussion or defer to recommendations on the subject by committees or reporters. In the latter case, however, (and this is our second reason), our data demonstrates a disconnect between directors and IT departments or reporters. This disconnect emerges as a result of: a) overly technical reporting (potentially leading to lay directors' disengagement with the topic), and b) insufficiently formalised reporting practices (potentially leading to sub-optimal cybersecurity decisions).

It is well acknowledged that while the technical nature of cybersecurity can be a barrier to understanding and engaging in this discipline (Soomro *et al.*, 2016), scarcely formalised cyber-reporting deserves further attention. We define the practice of giving reporters ultimate responsibility for what and how things are reported, as push reporting and argue that it makes formal authority ("the right to decide") differ from real authority ("the effective control over decisions") (Aghion & Tirole, 1997). Ultimately, this can translate into ill-informed cybersecurity decisions or board members' lack of control over performance (e.g., of a CISO).

Finally, our study offers insights into the established practice of delegating cybersecurity oversight to risk and audit committees. While this can reduce the burden on the entire board and increase competent cybersecurity discussions, evidence from other fields suggests that the quality of reporting to committees composed exclusively of NEDs is lower than reporting to the whole board (Adams *et al.*, 2021). The authority to make decisions on cybersecurity oversight still rests with a BoD as a whole; yet our study demonstrates that the latter obtains only very condensed and high-level information from risk and audit committees.

Which factors drive directors' engagement in cybersecurity (RQ2)?

Our study constitutes one of the first attempts to investigate the practices of cybersecurity in the boardroom. We relied on institutional theory in exploring the drivers for directors' engagement. Our investigation highlighted the compelling role of coercive pressures. Directors in highly regulated organisations engage more deeply in managing cyber-risks, at least to the extent required by their regulator. In the Australian case, Prudential Standard CPS234 (Australian Prudential Regulation Authority, 2019) emerged as particularly effective. However, prior research on organisational response to cyber-breaches (Jeyaraj & Zadeh, 2020) has demonstrated how the effect of coercive pressures tends to manifest primarily in the short term; questions could be raised around its effectiveness as a "maintenance therapy", especially when not coupled with other pressures in the same direction.

Directors' understanding and awareness of regulations affects the strength of coercive pressures: when a director is uncertain about their liability for cybersecurity oversight, the power of regulations is watered down. Even the directors that considered themselves operating in non-regulated entities would likely be responsible for cybersecurity, a responsibility conferred upon them by the Corporations Act 2001 (Australian Government, 2001; Australian Institute of Company Directors, 2021). In this sense, full delegation of cybersecurity duties to IT departments would contribute to moving cybersecurity "out of the boardroom", countering current literature (Rothrock *et al.*, 2018; Schinagl & Shahim, 2020). Our research demonstrates the need for strengthening Australia's cybersecurity regulations and clarifying liability for

***Corresponding Author:** Nonye Peter Awurum

cyber-governance and top management's involvement in cybersecurity (Australian Government, 2021).

Normative pressures also emerged as a significant driver, confirming prior literature (Vuko *et al.*, 2021). In fact, our respondents established that having a cybersecurity/IT background increases a director's confidence in addressing this topic, it promotes the debate within the boardroom, or renders such a director perceived as the subject matter expert by other directors. However, the degree of professionalisation normally entailed by normative forces was not present in our research, that is, no respondent either had or could identify in their BoDs other directors with formal certifications in cybersecurity (Columbus, 2020). Therefore, normative pressures can manifest in less formalised ways, i.e., based on experience. Interestingly, we discovered that normative forces could lead to perverse behaviours, such as an over-reliance on individual directors, who in turn may fear for their personal liability on cybersecurity matters.

Even though our investigation was not designed to compare the effectiveness of institutional pressures, mimetic pressures emerged as having the lowest impact on driving directors' engagement with cybersecurity. Directors holding positions in multiple companies are the most important source of mimicking the cybersecurity practices of other BoDs. Consulting firms were also indicated as potential drivers for mimetic pressures: consulting reports offer organisations an opportunity to measure their cyber-maturity (Siegel & Sweeney, 2020) against competitors (which often are clients of the same consulting firms, a phenomenon described as "cybersecurity monoculture" (Buckley *et al.*, 2019).

Besides the role of institutional pressures, other organisational factors emerged as promoting or hampering, directors' engagement with cybersecurity. We found that prior cyber-breaches strongly promote cybersecurity discussions in the boardroom. This confirms the findings by Jeyaraj and Zadeh (2020), who, however, considered prior cyber-breaches as a mere control variable in their institutional work on organisational responses to cyber-breaches.

Media reports about recent cyber-attacks also influence directors' engagement with cybersecurity in two opposite ways. On the one hand, they can help include cybersecurity in the agenda of BoDs, resulting in discussions that are rather informal. On the other hand, they can prompt comparisons with the attacked organisations, resulting in an "it won't happen to us" approach that epitomises the well-investigated optimism bias in cybersecurity (Pfleeger & Caputo, 2012).

Theoretical contribution and practical implications from our study

Our study casts light on the current engagement of directors with cybersecurity oversight, demonstrating that it is still in its infancy. This is mainly due to the technical nature of cybersecurity and to sub-optimal cyber-reporting practices ("push reporting"), which misalign formal authority from real authority (Aghion & Tirole, 1997).

We also contribute to neo-institutional theory through its novel application in the domain of cybersecurity governance at the top leadership level: coercive, normative and, to a lesser extent, mimetic pressures are key drivers in promoting directors' engagement with cybersecurity. An important role is also played by surrounding organisational factors.

Coercive (e.g., regulations) and normative pressures (e.g., education or practical experience in cybersecurity/IT; relatable media reports about eminent cyber-events) are particularly strong in driving directors' engagement with cybersecurity (AlKalbani *et al.*, 2017; Ogbanufe *et al.*, 2021; Vuko *et al.*, 2021). Mimetic pressures (e.g., external consultants, directors in multiple BoDs) due to a lack of information sharing dominating the cybersecurity discipline (Atapour-Abarghouei *et al.*, 2020) have a minor role. Organisational factors also importantly shape directors' engagement in cybersecurity through the impact of cyber-reporting practices ("push reporting"), the influence of prior cyber-attacks on the organisation (Jeyaraj & Zadeh, 2020), or the "dismissal" effect of unrelatable media reports about eminent cyber-events.

Significant, practical implications ensue. First, the current practice of delegating cybersecurity oversight to risk and audit committees needs to be accompanied by consolidated reporting practices (see organisational factors below) and clearer communication between the BoD and the committees.

Second, to leverage coercive pressures, regulations should clarify directors' responsibility for cybersecurity oversight. As an example, in Australia, the Corporations Act 2001 (Cth) (Australian Government, 2001) may already include this responsibility, but further clarification is required, as raised by a recent discussion paper (Australian Government, 2021) and some of its contributions (Australian Institute of Company Directors, 2021; Cyber Security Cooperative Research Centre, 2021).

Third, to strengthen normative pressures, the professionalisation of directors would positively affect their role in overseeing cyber-risk management: training in cybersecurity is an obvious option to partially fill the "background gap". Content-wise, we recommend training to be as holistic and business- and risk-focused as possible. As a mere example, directors do not need to be trained on the technicalities of a ransomware attack, but on the legal and managerial repercussions of system downtime, on the options for response and recovery, and on the implications of paying, or not paying, a ransom.

***Corresponding Author:** Nonye Peter Awurum

The creation of ad hoc cybersecurity certifications for board members is also a possibility. Hiring directors with proven experience in the field should be a priority. To the best of our knowledge, no country mandates this by law. As mere examples, the UK and the US are facing this same legislative vacuum. In the first case, GDPR is utilised as the reference regulation to raise boards and leaders' awareness towards cybersecurity. In parallel, toolkits and other 'soft' instruments have been created to support BoD's in their duties vis-à-vis cybersecurity (National Cyber Security Centre, 2021). As for the US, addressing the vacuum might just be a matter of time: in March 2022, the Securities and Exchange Commission (SEC) proposed legislation aimed at strengthening boards' engagement with cybersecurity by (among others) obliging them to include cyber-expertise in their ranks (Securities and Exchange Commission, 2022). An interesting parallel can be drawn between this rule proposal and the Sarbanes-Oxley Act, which, twenty years earlier, mandated disclosure of financial reporting expertise within BoDs in the country (Zukis, 2022).

Another priority should be to avoid having only one director with a cybersecurity background; this would avoid discharge of responsibility and/or complacency. Another option is the creation of "cybersecurity board champions", a diffused practice elsewhere in cybersecurity (Uchendu *et al.*, 2021).

Fourth, to leverage the long-term effect of mimetic pressures (Jeyaraj & Zadeh, 2020), it is important to multiply information and experience-sharing opportunities for directors on cybersecurity matters to promote the replication of best practices. Overarching institutions and associations (e.g., the Australian Institute of Company Directors) should play a leading role in this.

Fifth, to balance the influence of surrounding organisational factors, directors need to be supported to challenge, not just take note of, cyber-reports. To avoid the loss of "real authority" (Aghion & Tirole, 1997), guidelines should illustrate the most appropriate processes for reporting: that is, clear, bidirectional reporting lines (with directors' input on report contents, format, frequency, purposes, etc.; and their regular feedback on the quality and usability of the received reports), appropriate cyber-governance, and accountability structures, etc. For companies to set up their own reporting practices, we recommend adopting a design-led approach for the co-creation of reporting requirements by all the involved stakeholders (e.g., directors, CIO, CISO, Chief Risk Officer, Audit and compliance teams, IT departments, etc.) (Bongiovanni, 2020).

Sixth, opportunities to learn from cyber-events that have occurred in other organisations should be regularly organised in the boardroom with a focus on a detailed exploration of the circumstances (e.g., nature and size of the business, industry). Table 4 synthesizes the theoretical and the corresponding, practical contributions.

Table 4: Theoretical and practical contributions of the study

Theoretical contribution (and related RQ)	**Associated implications**	**Practical recommendations**
Expanded understanding of directors' engagement with cybersecurity: engagement is generally low (RQ1)	* Cybersecurity is still perceived as too technical; * "Push reporting" is a suboptimal practice: formal authority vs real authority * Practice of delegating cybersecurity oversight to risk and audit committees	* Consolidate cyber-reporting processes * Improve communication between BoDs and committees
Coercive pressures significantly promote directors' engagement with cybersecurity oversight (RQ2)		* Strengthen regulations and clarify directors' liability vis-à-vis cybersecurity oversight * Regulations mandating cyberexpertise in BoDs (e.g., Securities and Exchange Commission, 2022)
Normative pressures promote directors' engagement with cybersecurity oversight (RQ2)	* Professionalisation and addressing the cybersecurity background gap	* Cybersecurity training for directors * Ad hoc certifications

		* "Cybersecurity board champions"
Mimetic pressures marginally affect directors' engagement with cybersecurity oversight (RQ2)	* Secrecy typical of cybersecurity	* Information sharing opportunities for directors
Organisational factors affect directors' engagement with cybersecurity (RQ2)	* "Push reporting" * Prior cyber-breaches occurred to the organisation * Disengagement with eminent, unrelatable cyber-breaches	* Clear, bi-directional reporting lines * Consolidated reporting and accountability practices * Multiplication of learning opportunities from relatable cyber-breaches

Research Limitations and Areas for Future Research

In this study, we tackled the impenetrable "black box" of corporate boards (Watson *et al.*, 2020) and cast light on their engagement with cybersecurity. A first limitation could reside in the limited generalisability of our findings, typical of inductive research (Marshall & Rossman, 2011). In another location, this study could yield different results. However, two factors seem to minimise this concern: our conceptual framework is anchored in previous studies conducted in other jurisdictions; and the phenomena we described find correspondence in other countries (PwC, 2021; Securities and Exchange Commission, 2022). To overcome this limitation, we have carefully described our research approach to enhance its replicability (Shenton, 2004) and invite other researchers to replicate our study elsewhere for a comparison of results. To increase the generalisability of our findings (Billups, 2020), we recommend crafting a quantitative research project (e.g., a survey) investigating the same research questions.

Another limitation is associated with our purposeful sampling, which could have led to sampling bias (Patton, 2015). Our participants were interested in our study as it was seen by many of them as an opportunity to learn more about cybersecurity. This could have made them non-representative of typical NEDs. Nevertheless, they provided honest, self-critical accounts of their experiences (including an acknowledged lack of understanding of cybersecurity). Furthermore, 43 organisations were represented in our sample, expanding its representativeness. To further overcome this limitation, future qualitative research could be designed for a "deep dive" into a limited number of boards, increasing the number of interviewed directors per board.

CONCLUSION

The growth in number and scale of cyber-breaches occurring to public and private sector organisations worldwide has recently multiplied calls in both literature and practice for an enhanced, more proactive role by BoDs in cybersecurity oversight. Despite this, there have been limited studies that have investigated current practices for directors to engage in the cybersecurity domain. Even less focus has been on what drivers could influence such engagement. Anchored in neo-institutional theory, our study addresses these two gaps: on the one hand, it expands our knowledge of cyber-governance practices at the BoD level by demonstrating that, overall, directors' commitment to cybersecurity is still scarce; on the other hand, it analyses the drivers that shape these dynamics. From this novel body of evidence, we draw a series of practical recommendations that promote an incontrovertible matter of fact, namely that directors need to increase their engagement in cybersecurity oversight.

REFERENCES

1. Abu-Musa, A. (2010). Information security governance in Saudi organizations: An empirical study. *Information Management & Computer Security, 18*(4), 226–276. https://doi.org/10.1108/09685221011079180
2. Adams, R. B., Ragunathan, V., & Tumarkin, R. (2021). Death by committee? An analysis of corporate board (sub-) committees. *Journal of Financial Economics, 141*(3), 1119–1146. https://doi.org/10.1016/j.jfineco.2021.05.032
3. Aghion, P., & Tirole, J. (1997). Formal and real authority in organizations. *Journal of Political Economy, 105*(1), 1–29.
4. Aguilar, L. A. (2014). *Boards of directors, corporate governance and cyber-risks: Sharpening the focus*. https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/jun2014/cs06102014_BOD_Corporate_Governance_Cyber_Risks.pdf
5. AlKalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information security compliance in organizations: An institutional perspective. *Data and Information Management, 1*(2), 104–114. https://doi.org/10.1515/dim-2017-0006
6. Ando, H., Cousins, R., & Young, C. (2014). Achieving saturation in thematic analysis: Development and refinement of a codebook. *Comprehensive Psychology, 3*, Article 03.CP.03.04.

***Corresponding Author:** Nonye Peter Awurum

7. ASX Corporate Governance Council. (2019). *Corporate governance principles and recommendations* (4th ed.). https://www.asx.com.au/documents/asx-compliance/cgc-principles-and-recommendations-fourth-edn.pdf
8. Atapour-Abarghouei, A., McGough, S., & Wall, D. S. (2020, December 10–13). Resolving the cybersecurity data sharing paradox to scale up cybersecurity via a co-production approach towards data sharing. In *Proceedings of the IEEE International Conference on Big Data (Big Data 2020)*. IEEE.
9. Australian Cyber Security Centre. (2021). *ACSC annual cyber threat report 2020–2021*. https://www.cyber.gov.au/sites/default/files/2021-09/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf
10. Australian Government. (2021). *Strengthening Australia's cyber security regulations and incentives: An initiative of Australia's cyber security strategy 2020*. https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf
11. Australian Institute of Company Directors. (2020). How to fix the skills gap in the boardroom. *Australian Financial Review*. https://www.afr.com/work-and-careers/careers/how-to-fix-the-skills-gap-in-the-boardroom-20201207-p56ldj
12. Australian Institute of Company Directors. (2021). *Submission: Strengthening Australia's cyber security regulation and incentives*. https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/australian-institute-of-company-directors-aicd.pdf
13. Australian Institute of Company Directors, & Roy Morgan. (2021). *Director sentiment index survey: 2nd half 2021*. https://aicd.companydirectors.com.au
14. Australian Prudential Regulation Authority. (2019). *Prudential standard CPS 234: Information security*. https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf
15. Babbie, E. R. (2013). *The practice of social research* (13th ed.). Cengage Learning.
16. Bajra, U., & Čadež, S. (2018). Audit committees and financial reporting quality: The 8th EU Company Law Directive perspective. *Economic Systems, 42*(1), 151–163.
17. Billups, F. D. (2020). *Qualitative data collection tools: Design, development, and applications*. Sage Publications.
18. Boehm, J., Curcio, N., Merrath, P., Shenton, L., & Stahle, T. (2019). *The risk-based approach to cybersecurity*. McKinsey & Company. https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity
19. Bongiovanni, I. (2020, December 2). Designing user-centric information security management systems in financial services organisations. In *HACS2020 Conference Proceedings*.
20. Buckley, R. P., Arner, D. W., Zetzsche, D. A., & Selga, E. (2019). The dark side of digital financial transformation: The new risks of FinTech and the rise of TechRisk. *UNSW Law Research Paper*, 19–89.
21. Center for Strategic and International Studies. (2021). *Significant cyber incidents*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
22. Cohn, Y., Kelley, K. H., & Nasdaq. (2017). Fulfilling the board's cyber risk oversight role: A practical guide. *The Corporate Governance Advisor, 25*(5), 23–30.
23. Columbus, L. (2020, June 16). Top 10 most popular cybersecurity certifications in 2020. *Forbes*. https://www.forbes.com/sites/louiscolumbus/2020/06/16/top-10-most-popular-cybersecurity-certifications-in-2020/
24. Cyber Security Cooperative Research Centre. (2021). *Submission on strengthening Australia's cyber security regulations*. https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/cyber-security-cooperative-research-centre.pdf
25. Damenu, T. K., & Beaumont, C. (2017). Analysing information security in a bank using soft systems methodology. *Information and Computer Security, 25*(3), 240–258. https://doi.org/10.1108/ICS-07-2016-0053
26. DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147–160.
27. Enterprise Strategy Group. (2020). *Cybersecurity in the C-suite and boardroom*. https://www.bitsight.com/resources/cybersecurity-in-the-c-suite-and-boardroom
28. European Banking Authority. (2019). *Guidelines on ICT and security risk management*. https://www.eba.europa.eu
29. EY, & Institute of Internal Auditors. (2021). *The risky six: Key questions to expose gaps in board understanding of organisational cyber resiliency*. https://global.theiia.org
30. Federation of European Risk Management Associations. (2018). *Cyber risk governance report*. https://www.ferma.eu
31. Gartner. (2021). *Forecasts worldwide security and risk management spending*. https://www.gartner.com
32. Grobman, S., & Cerra, A. (2016). *The second economy: The race for trust, treasure, and time in the cybersecurity war*. Apress.

33. Haislip, J., Lim, J., & Pinsker, R. (2017, August 10–12). Do the roles of the CEO and CFO differ when it comes to data security breaches? In *Proceedings of the Americas Conference on Information Systems*.
34. Hartmann, C. C., & Carmenate, J. (2021). Academic research on the role of corporate governance and IT expertise in addressing cybersecurity breaches. *Current Issues in Auditing, 15*(2), A9–A23. https://doi.org/10.2308/CIIA-2020-034
35. Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies. *Decision Sciences, 43*(4), 615–659. https://doi.org/10.1111/j.1540-5915.2012.00362.x
36. Jeyaraj, A., & Zadeh, A. (2020). Institutional isomorphism in organizational cybersecurity. *Journal of Organizational Computing and Electronic Commerce, 30*(4), 361–380. https://doi.org/10.1080/10919392.2020.1776033
37. Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce, 28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598
38. Kosseff, J. (2019). *Cybersecurity law*. Wiley.
39. Kvale, S. (1996). *Interviews: An introduction to qualitative research interviewing*. Sage.
40. Lacroix, K. (2016). Target Corporation cybersecurity-related derivative litigation dismissed. *The D&O Diary*. https://www.dandodiary.com
41. Landefeld, S. M., Mejia, L. R., & Handy, A. C. (2015). Board tools for oversight of cybersecurity risk. *The Corporate Governance Advisor, 23*(3), 1–10.
42. Lankton, N., Price, J. B., & Karim, M. (2021). Cybersecurity breaches and IT governance. *Journal of Information Systems, 35*(1), 101–119. https://doi.org/10.2308/isys-18-071
43. Lawrence, T. B., & Shadnam, M. (2008). Institutional theory. In W. Donsbach (Ed.), *The international encyclopedia of communication*. Wiley.
44. Leblanc, R., & Fraser, J. R. S. (2016). *The handbook of board governance*. Wiley.
45. Leech, T., & Hanlon, L. (2016). Three lines of defense versus five lines of assurance. In R. Leblanc & J. Fraser (Eds.), *The handbook of board governance* (pp. 335–355). Wiley.
46. Leszczyna, R. (2018). Cybersecurity standards for smart grids. *Computers & Security, 77*, 262–276. https://doi.org/10.1016/j.cose.2018.03.011
47. Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage.
48. Marshall, C., & Rossman, G. B. (2011). *Designing qualitative research* (5th ed.). Sage.
49. Martin, S. (2014). Cyber security: 60% of techies don't report breaches. *International Business Times*. https://www.ibtimes.co.uk
50. Miles, M. B., & Huberman, A. M. (1984). Drawing valid meaning from qualitative data. *Educational Researcher, 13*(5), 20–30. https://doi.org/10.2307/1174243
51. MinterEllison. (2020). *Perspectives on cyber risk*. https://www.minterellison.com
52. Mishra, S. (2015). Organizational objectives for information security governance. *Information & Computer Security, 23*(2), 122–144.
53. National Association of Corporate Directors, & Internet Security Alliance. (2020). *Cyber-risk oversight 2020*.
54. National Cyber Security Centre. (2021). *Cyber security toolkit for boards*. https://www.ncsc.gov.uk
55. Ogbanufe, O., Kim, D. J., & Jones, M. C. (2021). Cybersecurity strategic commitment. *Information & Management, 58*(7), 103507. https://doi.org/10.1016/j.im.2021.103507
56. Patton, M. Q. (2015). *Qualitative research & evaluation methods* (4th ed.). Sage.
57. Pfleeger, S. L., & Caputo, D. D. (2012). Behavioral science in cybersecurity. *Computers & Security, 31*(4), 597–611.
58. PwC. (2021). *Annual corporate directors survey*. https://www.pwc.com
59. RedSeal. (2016). *Cyber-overconfidence in the C-suite*. https://www.redseal.net
60. Renaud, K., Von Solms, B., & Von Solms, R. (2019). Intellectual capital and cybersecurity. *Journal of Intellectual Capital, 20*(5), 621–641. https://doi.org/10.1108/JIC-04-2019-0079
61. Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review, 59*(2), 12–15.
62. Schinagl, S., & Shahim, A. (2020). Information security governance. *Information and Computer Security, 28*(2), 261–292.
63. Scully, T. (2014). The cybersecurity threat stops in the boardroom. *Journal of Business Continuity & Emergency Planning, 7*(2), 138–148.
64. Shenton, A. K. (2004). Trustworthiness in qualitative research. *Education for Information, 22*(2), 63–75.
65. Siegel, C. A., & Sweeney, J. M. (2020). *Cyber strategy: Risk-driven security and resiliency*. Auerbach.
66. Soomro, Z., Shah, M., & Ahmed, J. (2016). Information security management: A literature review. *International Journal of Information Management, 36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009
67. Stake, R. E. (1995). *The art of case study research*. Sage.
68. Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis, 76*, 101795. https://doi.org/10.1016/j.irfa.2021.101795
69. Tripwire. (2019). *The language of risk*. https://www.tripwire.com

***Corresponding Author:** Nonye Peter Awurum

70. Tsen, E., Ko, R. K., & Slapničar, S. (2022). Organizational cyber resilience. *Journal of Organizational Computing and Electronic Commerce*.
71. Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cybersecurity culture. *Computers & Security, 109*, 102387.
72. Valentine, E. L. H., & Stewart, G. (2013). Board role in IT governance. *International Journal of Disclosure and Governance, 10*(4), 346–362. https://doi.org/10.1057/jdg.2013.11
73. Von Solms, B., & Von Solms, R. (2018). Cybersecurity vs information security. *Information & Computer Security, 26*(1), 2–9.
74. Von Solms, R., & Von Solms, B. (2006). Information security governance: Due care. *Computers & Security, 25*(7), 494–497. https://doi.org/10.1016/j.cose.2006.08.013
75. Watson, C., Husband, G., & Ireland, A. (2020). Governance processes. *Journal of Management and Governance, 25*(1), 189–221. https://doi.org/10.1007/s10997-020-09503-3
76. Yin, R. K. (2009). *Case study research: Design and methods* (4th ed.). Sage.
77. Zattoni, A., Douglas, T., & Judge, W. (2013). Corporate governance theory. *Corporate Governance: An International Review, 21*(2), 119–122. https://doi.org/10.1111/corg.12016
78. Zukis, B. (2016). Information technology and cybersecurity governance in a digital world. In R. Leblanc (Ed.), *The handbook of board governance* (pp. 555–573). Wiley. https://doi.org/10.1002/9781119245445.ch28
79. Zukis, B. (2022, April 18). The SEC is about to force CISOs into America's boardrooms. *Forbes*. https://www.forbes.com/sites/bobzukis/2022/04/18/the-sec-is-about-to-force-cisos-into-americas-boardrooms/