UTS UNIVERSITY OF TECHNOLOGY SYDNEY

Cybersecurity Governance Framework for Board Directors

by Sarvjit Singh Girn

Thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy (CO2029)

under the supervision of Professor Asif Q. Gill, Head of Discipline (Software Engineering), UTS

Co-Supervisor: Professor Ghassan Beydoun, Head of Discipline (Information Systems), UTS

External-Supervisor: Distinguished Professor Willy Suliso, Director of Cybersecurity and Cryptology, University of Wollongong

University of Technology Sydney
Faculty of Engineering and Information Technology

December 2024

CERTIFICATE OF ORIGINAL AUTHORSHIP

I, Sarvjit Singh Girn, declare that this thesis is submitted in fulfilment of the requirements for the award of Doctor of Philosophy in the Faculty of Engineering and IT, School of Computer Science at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Production Note:
Signature removed prior to publication.

8th December 2024

Directors have a critical role to play and must seek to lift their own cyber literacy levels, recognising that this is a key risk that can never be eliminated but can be effectively managed.

Hon Clare O'Neil MP
Minister for Home Affairs and Minister for Cyber Security, Australian Government

Table of Contents

List of Figures

List of Tables

i. Copyright statement

ii. Abstract

The importance and necessity of managing cybersecurity risk has become more relevant as the dependency on online digital services has grown for many organizations. This is compounded by the fact that threats to the digital economy and overarching operational resilience have increased, and continue to do so, in sophistication and volume. In particular, governing for cybersecurity resilience is a critical imperative in this environment. Board Directors and Senior Executives are apprehensive when it comes to governing the quality of their organization's cybersecurity. Cybersecurity for many senior business audiences is challenging given the technical language in use and the ever-changing nature of the field as new intricate threats evolve in digital platforms. Whilst in recent years there has been a growth in awareness on the importance of cybersecurity at the Board level, there has been a lack of practical frameworks and models to guide such stakeholders. Thus, this thesis aims to address the important research question of "*What framework should be developed to help non-technical audiences such as Board Directors and Senior Executives better govern cybersecurity?"* This thesis proposes a novel framework, which is called the Board Cybersecurity Governance Framework (BCGF). This framework consists of seven related models: Assets, Risk Appetite Statement, Standards, Risk Clusters, Metrics, Questions and Culture which are designed to support Board-level cybersecurity governance. The proposed framework and underpinning models were iteratively developed and evaluated using the design science research method. The initial version of the framework was developed based on the literature review. This framework was further developed through design workshops and interviews with 15 Board Directors and related senior stakeholders. An expert evaluation workshop and an associated online survey with 20 experienced stakeholders were conducted to evaluate and refine the proposed framework. The evaluation results indicate that the proposed framework is appropriate for Board Directors and Senior Executives aiming to govern cybersecurity. While the proposed framework addresses the current research question in hand as a part of the applied research and innovation program, it is important to acknowledge the dynamic nature of the cybersecurity field, which will warrant the continuous evolution and adaptation of the framework for different organisational contexts.

iii. Acknowledgements

I would like to recognise the support, guidance and constructive feedback provided by my supervisors over the course of this research. Professor Asif Gill has been a pillar of support in challenging my thinking, guiding the research process, and offering the right encouragement when I needed it most to continue this important research for Board Directors. Professor Ghassan Beydoun and Distinguished Professor Willy Suliso have provided invaluable input into assessments and detailing the importance of rigour in the research process.

My heartfelt acknowledgement to my own family who have offered their support and allowed me many days and weeks away to focus on this study over the years. Without this, the research would not have been completed. My extended family of friends has also been a source of encouragement, that has driven me to conclude the work and then share it more broadly in industry and academic networks.

I would also like to acknowledge the support of the Australian Government, who supported this research through the Australian Government Research Training Program. I hope the application of this research gives more confidence to Board Directors and Senior Executives in their responsibility of governing cybersecurity risk for their organizations.

iv. List of Abbreviations

Abbreviation	Description
AICD	Australian Institute of Company Directors
ACSC	Australian Cyber Security Centre
APRA	Australian Prudential Regulatory Authority
ASIC	Australian Security and Investments Commission
BCGF	Board Cybersecurity Governance Framework
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operations Officer
CRO	Chief Risk Officer
CXO	Chief Officer (Senior Executive reporting to the Chief Executive Office)
DSR	Design Science Research
GT	Grounded Theory
NED	Non-Executive Director
RMF	Risk Management Framework
SME	Subject Matter Expert

v. List of Publications and Presentations

Table 1 outlines the engagement in academic, business, and industry forums on the research topic in recent years and one that is planned.

Ref#	Industry Conferences & Workshops	Date
1.	Digital Identity & Security in the Health Sector, "The Future of Technology, Innovation & Work Conference" 6Degrees.AI, Sydney	November 2022
	Board Presentations as a Senior Executive	
2.	Cuscal Payments Board – 'Cybersecurity Education'	October 2021
3.	I-MED Radiology Network Board – 'Cybersecurity Update'	April 2022 – present (quarterly)
4.	Reserve Bank of Australia – 'Cybersecurity Update'	June 2012 – May 2018 (quarterly)
	Cybersecurity Governance as a Board Member	
5.	Reserve Bank Health Society, Audit and Risk Committees	2014-23 (quarterly)
6.	Can Too Foundation, Audit and Risk Committee	2016 – present (quarterly)
7.	Commonwealth Bank Health Society, Audit and Risk Committees	October 2023 – present (quarterly)
8.	Police Bank, Audit and Risk Committees	November 2023 – present (quarterly)
	Academic Conferences & Workshops	
9.	A Data-Driven Approach to Board Cybersecurity Governance. Pacific Asia Conference on Information Systems 2022 (PACIS) - (Girn, 2022)	April 2022
10.	Board Cybersecurity Framework, Cybersecurity at MIT (CAMS) Conference, Boston, USA	July 2023
11.	Board Cybersecurity Framework, UTS FEIT Education & Government Conference, Sydney	October 2023
12.	IEEE Technology and Society Magazine	Planned to be submitted. In progress.
	Media Interviews	
13.	Digital Nation Australia Boardroom Impact, NextMedia, Interview on Cybersecurity for Board Directors. https://www.itnews.com.au/video/cover-story-technology-alone-cant-beat-cybercrime-attack-the-economic-triggers-say-cisos-577648	March 2022
	Journals	
14.	IEEE Transactions on Technology and Society	Final research planned to be submitted. Work in progress.

Table 1: Publications and presentations

1 Introduction

The importance and need to manage cybersecurity risk has become more relevant as the dependency on online digital services has grown for many organizations. This is compounded by the fact that threats to the digital economy and overarching operational resilience have increased, (and continue to do so), in sophistication and volume. In particular, governing cybersecurity risk is a critical imperative in this environment. Board Directors (Non-Executive Directors, NED) and Senior Executives (Chief Executive Officers, CXO) are apprehensive when it comes to governing the quality of their organization's cybersecurity. Cybersecurity for many senior business audiences is challenging given the technical language in use and the ever-changing nature of the field as new intricate threats evolve in technology platforms. Whilst there has been a growth in awareness at a principle level, there is a lack of research-based practical frameworks and models to guide such stakeholders. This is analysed in detail in Chapter 2 (Research Background and Problem). Further, regulators and governments have recognised the importance of cybersecurity resilience to protect the interests of consumers and the viability of organizations themselves. In many jurisdictions legal penalties have been applied to individuals and companies that do not adequately govern the posture of cybersecurity (ASIC, 2020). This has placed more onus on Board Directors to focus on such risks. Prior literature aimed at NEDs and CXOs has been examined through a review of reputable academic and business sources. Pain points, aspirations, and knowledge-gaps amongst NEDs and CXOs have been identified through interviews. This thesis provides a solution (the BCGF) to assist non-technical audiences such as Board Directors and Senior Executives to better govern cybersecurity risk. The BCGF consists of a series of 7 related models which provide new and novel tools that can be applied in a practical way in various scenarios in Board cybersecurity risk management governance. Design science research, augmented with grounded theory techniques, have been applied to develop and evaluate this framework. The framework will provide a systematic approach and guidance to NEDs and CXOs aiming to govern cybersecurity in their organisations. It enables an approach that can be tailored to the unique risk profile of an organization and provide a guide to the non-technical audience.

This chapter provides an overview of the research problem and the manner in which the solution has been derived and evaluated. It first establishes a baseline of definitions in cybersecurity and cybersecurity governance. It then provides context to the threat landscape that is raising awareness of the importance of governing cybersecurity risk, and then explains the challenges or problems that NEDs and CXOs face in this critical imperative. The research gap is outlined, along with a research strategy to address this gap. Finally, an overview of the proposed solution (the BCGF) informed by this research is presented.

1.1 Research Background and Context

This research is conducted on the main topic of cybersecurity governance that targets the Board of Directors and Senior Executives that report to them. This is deemed an important stakeholder group, as they are the custodians of setting the strategy, tone, and risk levels for the organization at large. The research references NEDs and CXOs, however this is also relevant and applicable to the public sector, where such roles have other titles, such as Department Head or First Secretary, with equivalent governance responsibilities. A critical stage in this research is first understanding the definitions of cybersecurity and cybersecurity governance, which are terms that have their own unique and varied interpretation to various stakeholders.

1.1.1 Cybersecurity

The term "cybersecurity" is used in many contexts and often has different meanings for authors and stakeholders that need to then interpret their writings. For this research, a broad definition of cybersecurity is adopted, namely 'the protection of technology systems from unauthorized access

through a range of protection measures covering people, processes and technology, that safeguard the confidentiality, integrity and availability of the systems themselves, and information held within them'. This definition is informed by several viewpoints detailed in the literature review in Chapter 3 , including (Azmi et al., 2018; Cebula et al., 2014; Craigen et al., 2014; von Solms & van Niekerk, 2013). The adopted definition enables the inclusion of soft elements, such as people, culture, and behaviour (dealing with a social engineering threat), along with hard elements such as policy, standards, and technology (dealing with the technical aspects in systems).

The variability in the definition of cybersecurity has forced many authors to state an assumed definition upfront to minimise ambiguity (Azmi et al., 2018). Some authors such as (Craigen et al., 2014) have argued the case that definitions are varied and that the multidimensions of cybersecurity are not captured in any existing definition. For example, (Rout, 2015) argues that the situation is difficult as industry, business, and academics are unable to agree on trivial issues such as whether its 'cybersecurity' (one word) or 'cyber security' (two words), and there is also confusion with the relationship with 'information security' coming into play. This is where the general view of cybersecurity being broader than information security is argued by (von Solms & van Niekerk, 2013) who debate that many elements of cybersecurity sit outside of information security. Some such as (Cains et al., 2021) argue that current definitions are "inadequate due to lack of inclusion of human factors, no standardized cyber security terminology exists across disciplines". However, there is a convergence in views (Cebula et al., 2014), where cybersecurity is seen as not simply limited to the technology or process domains required to maintain it. It also encompasses other aspects, such as human behaviour and organization culture. It is often seen as being associated with the way people compromise systems for data theft and intelligence, and the required protection mechanisms to prevent this. An example of this is social engineering to compromise systems, which may be minimised through a focus on security culture and awareness. One aspect that may have contributed to the confusion in the definition of the cybersecurity could be the fact that the use of the term in various references only stems from the mid-to-late 1990s as shown in the Ngram[1] in Figure 1. In this figure, the use of the term coincides with the broader adoption of the public internet and a growth of commercial online services that drew the attention of criminals from the late 1990s, an example of this being, internet banking in Australia, which was launched by banks in a similar period of time.

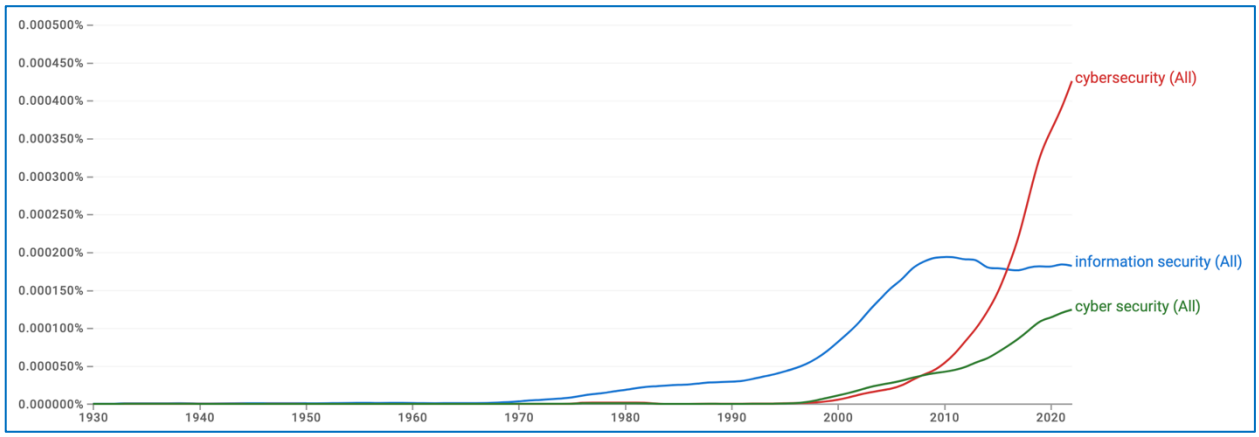

Figure 1: Google ngram viewer - 'cyber security, cybersecurity & information security'(1930-2022)

Further detail on cybersecurity definitions and various concepts covered by these definitions is discussed in Section 2.2.

1.1.2 Cybersecurity Governance

[1] The Ngram viewer is a tool provided by Google, which enables the search of published books until 2019. This should not be taken as an accurate picture of occurrences; it is used here purely as an indicative element and does not replace the rigour of a literature review.

Following on from the definition of cybersecurity in the previous section, it becomes important to understand the way cybersecurity is governed in terms of overseeing and directing investments and resources towards the desired maturity. This oversight, or 'governance' was explained by (Allen, 2005) as "setting clear expectations for the conduct (behaviours and actions) of the entity being governed, and directing, controlling and strongly influencing the entity to achieve these expectations". In the context of cybersecurity governance, this is often stated as the activities to align the maturity of cybersecurity (and sustain this) to the desired standard to support the business goals and strategies (AlGhamdi et al., 2020). There are a number of facets in governance, including setting policy, authority, control, influencing and regulating the entity in question. The literature generally covers three foundational elements, namely the *oversight* required to ensure the right cybersecurity maturity, the *frameworks* that can be used to apply this authority, and finally the *compliance* elements necessary to provide assurance to various stakeholders. These facets are now briefly discussed here.

Oversight of cybersecurity begins at the Board level, with the setting of business strategy and goals, along with defining and embedding a risk framework to guide the risk appetite and delivery. The need for this oversight is cited by (AlGhamdi et al., 2020; Bruin & Solms, 2016) who emphasise the need for Board level and top-level management focus to drive maturity. This is also the theme amongst regulators, who in recent years have held Boards responsible for the posture of cybersecurity risk (APRA, 2019). *Frameworks* play a critical guiding role in the governance and implementation of processes and controls for cybersecurity. The Information Security Governance and Management (ISGM) framework from (Carcary et al., 2016) has its basis in COBIT (Harmer, 2013) and the Open Group (OpenGroup, 2017). Similarly, security standards from ISO, such as (ISO, 2018), (ISO, 2013a) and (ISO, 2013b) highlight the key processes and controls expected in best practice organizations. Whilst these frameworks and standards are comprehensive and drive a greater focus on strengthening security, they are focussed on the security or risk practitioners and have an inherent level of assumed technical knowledge in this domain. NEDs and CXOs are not well served in this regard as they may not have detailed technical knowledge of cybersecurity. The cybersecurity and risk expert is the target audience for many of these existing framework and standards (Girn, 2022). Furthermore, *compliance* has assumed an important role in recent years. Regulated entities, especially those that represent critical infrastructure such as banking, utilities, and transport, have faced increased scrutiny on the posture of their cybersecurity given the impact on the broader economy and the public from a breach of security. By way of example, the Australian Securities and Investment Commission (ASIC) published a range of standards for companies on good cybersecurity resilience, including (ASIC, 2015). It has, over time, increased its focus through additional reviews of the corporate sector to highlight good practices and areas for improvement (ASIC, 2019). Similar to frameworks, the importance and need for adequate compliance with these standards is not supported by practical advice and guidance that NEDs and CXOs can apply to their organisations. This indicates the need for research in this important area of cybersecurity governance at Board and Senior Executive levels. Further details on cybersecurity governance and the key elements are discussed in Section 2.4.

1.1.3 Research Context

The importance of managing cybersecurity risk has become more relevant as the dependency upon online digital services has grown for many organizations, and as threats to the digital economy have increased in sophistication and volume (ACSC, 2022; Li & Liu, 2021). Modern economies are dependent on the continued availability of online digital services, with many required to operate on a 24x7 basis. Cybersecurity resilience is the capacity of an organization to withstand, recover from and adapt to the impacts causes by cybersecurity incidents (Dupont et al., 2023). It is seen as a subset of cybersecurity and places focus on activities for recovery from an incident, which complement the usual activities to protect the organization (Coden et al., 2023; Proudfoot et al., 2023). This has become an important requirement in terms of the confidentiality, integrity and availability of digital services within the broader context of business continuity (SCC/SEC, 2023). Consumers have become more aware of the need for and importance of organizations to protect their data and have demanded a speedy response

and action when faced with data breaches that have exposed their personal data. This requires consumers to make arrangements for new identity documents, such as driving licenses, with subsequent class actions being triggered against compromised organizations (OPTUS, 2023). Regulators and governments have recognised the importance of cybersecurity resilience to the economy and protecting the interests of consumers and the public at large. In many jurisdictions and sectors, legal penalties have been imposed on individuals and companies that do not adequately govern the posture of cybersecurity (ASIC, 2020). This has more recently included fines and additional capital requirements in regulated industries such as financial services (APRA, 2023). NEDs and CXOs are apprehensive when it comes to governing the quality of their organization's cybersecurity with only 50% of Boards somewhat confident that their company is adequately secured against cybersecurity attacks (ASX/ASIC, 2017). There has been a growth in awareness in recent years, coupled with increasing principle-level guidelines. However, these have remained at a conceptual level as can be seen from the risk report from the World Economic Forum (WEF, 2021). A lack of good and appropriate cybersecurity governance threatens a number of organizations in maintaining a sound cybersecurity posture. However, if cybersecurity risk is handled well in a structured and informed manner, this can become a competitive differentiator in the modern digital economy (Kosutic & Pigni, 2021).

1.2 Problem Statement

While there is an increasing awareness and interest in cybersecurity in recent times due to the threat landscape (Li et al., 2019; Pienta et al., 2020). The challenges around cybersecurity governance however remain prevalent as depicted in the problem statement in Figure 2. This highlights a research gap in organizations between those stakeholders that govern and lead the posture of cybersecurity from the top, and those that are responsible for the implementation and operations of cybersecurity controls within it. This is made more challenging, given the threats continue to grow in sophistication and volume and they consequently have an adverse impact on organisations as seen in a number of successful attacks (Li et al., 2019; OPTUS, 2023; Pienta et al., 2020). Further, due to an ongoing emergence of updated/new industry/business regulations, policies, and standards, the environment becomes more complex in assurance and compliance (Haislip et al., 2021; Walton et al., 2021). This is compounded by the evolution of new technology and digital solutions that need to be understood (Brown et al., 2017; Walton et al., 2021).

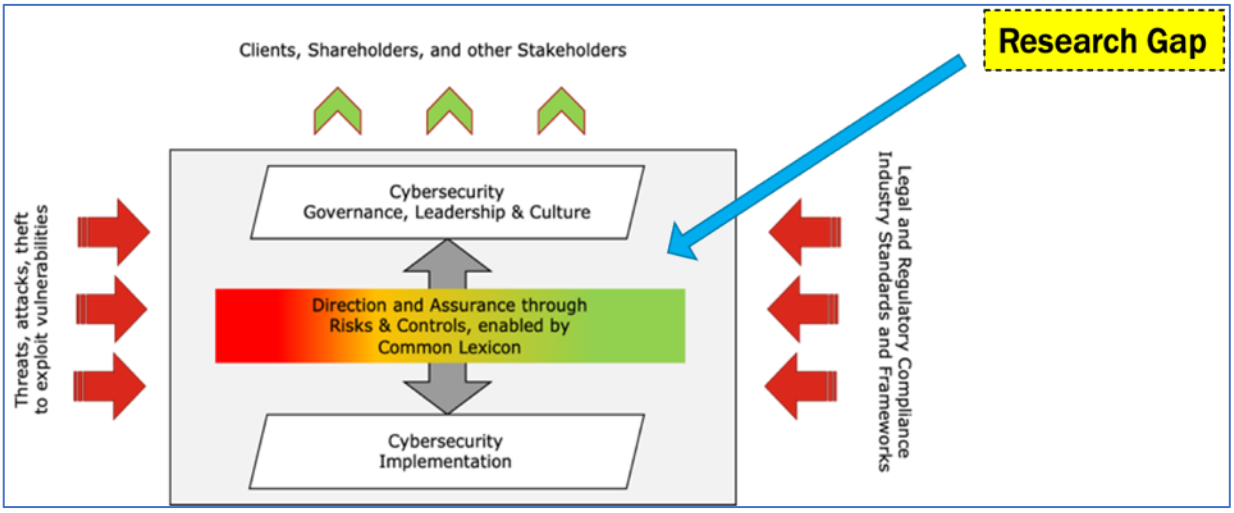

Figure 2: Cybersecurity governance context

The compliance requirements and guidelines are mostly high level, with linkages to the underlying technical cybersecurity posture being undefined or left to each organization to derive (this is addressed in the literature review in Chapter 3). At the other end of the spectrum, standards are targeted at a technical audience for ease of implementation, with limited business lexicon to align to the principles and intent of risk appetite statements of Boards and other governing bodies. The variability in the

definition of cybersecurity across dictionaries, literature, industry, and business has created ambiguity in its scope with stakeholders (Cains et al., 2021; Craigen et al., 2014; Rout, 2015; von Solms & van Niekerk, 2013). The definition includes not just technical dimensions, but also aspects such as culture, processes, and people. The problem exists in the gap between those that govern and lead the cybersecurity risk posture, and those that are responsible for the implementation of strategies and technologies in the environment in this context (Girn, 2022). This gap is seen in a lack of common frameworks, models, language, and approaches that can help bridge the non-technical and technical divide amongst Board Directors and the Senior Executives that report into them (Iden & Eikebrokk, 2013; Lee et al., 2016). The problem stems from the fact that many of these stakeholders are not adept in cybersecurity governance due to the complex and ever-changing nature of this field. Whilst principles and general guidance have been provided to these audiences by relevant regulators, there is a distinct lack of a research targeted at the Board Director and Senior Executive. This is further covered in detail in the literature review in Chapter 3.

The research gap is seen in a lack of literature, such as frameworks and models, that focus on business stakeholders, such as Board Directors and Senior Executives, in a non-technical language (Girn, 2022). This is further covered in Chapter 2 (Research Background and Problem). There is limited guidance to such stakeholders. This gap has in many instances led to two broad outcomes. The first is a potential weakness in the cybersecurity posture of an organization stemming from a lack of understanding at a governance and strategy level, a case in point being reported in the ASX Cyber Health Check Report which stated that only 34% of the ASX 100 companies surveyed indicated they have clearly defined and understood their cybersecurity risk appetite (ASX/ASIC, 2017). The second is a potential over-investment in general terms, and not focusing on protecting the assets that really matter in terms of the business data and operational resilience needs of the organization (Safi et al., 2021). This research gap leads to the following core Research Question (RQ).

RQ: *What framework should be developed to help non-technical audiences such as Board Directors and Senior Executives better govern cybersecurity?*

This main research question is further decomposed into sub-questions. More detail on the specific sub-questions, and the aims and deliverables for these are in Section 2.7.

1.3 Aim and Scope

The scope of this research is targeted towards Board Directors and Senior Executives, as stakeholders that must govern cybersecurity risk at the senior most levels in an organisation. There are linkages from these stakeholders to roles that are accountable for implementing cybersecurity, including CIOs, CISOs, CROs and other subject matter experts (SMEs). These linkages are important, and the research examines how to provide more clarity in the two-way exchange between stakeholders of information such as, setting standards, agreeing on the risk appetite, establishing the right cybersecurity culture, asking insightful questions, and establishing the right metrics to monitor cybersecurity health. The aim of the research is to identify the gaps observed in the literature available to Board Directors and Senior Executives, and the pain points and aspirations they have when governing cybersecurity. Examples include guidance to identify which critical assets an organization needs to protect, determination of the cybersecurity risk appetite statement, and practical ways to educate themselves of evolving cybersecurity concepts. Following on from identification and synthesis of the gaps, the aim of the research is to formulate a practical cybersecurity framework that consists of a series of models to help address these gaps. It is anticipated that this resulting framework will help them to govern cybersecurity risk more effectively and in a systematic manner that is grounded on specific data inputs to guide Board discussions and outcomes.

1.4 Research Significance

This research is important and timely because Board-level governance is critical for managing the security posture of an organization (AICD, 2022a, 2022b, 2024b; APRA, 2023; SCC/SEC, 2023), there is a lack of research and knowledge on how to govern the cybersecurity at the Board level (Kappelman et al., 2020; Nolan & McFarlan, 2005), and there are increasing regulations and reporting requirements that warrant effective cybersecurity governance at the Board level (Haislip et al., 2021; Walton et al., 2021).

The framework will allow leaders to be more confident of the security posture, through the use of specific models (with relevant inputs, activities and outcomes) to assist them. This is akin to the financial accounting frameworks and data that enable leaders to exercise their fiduciary responsibilities when running organisations. This will also increase the knowledge of cybersecurity for this audience so they will become more informed to ask the right questions, and then set the tone of what is expected with more confidence. This can only be a good thing if it results in the better protection of the digital assets of organizations as they relate to their services, products, customers, and data. Furthermore, the framework will be made available to Boards and Senior Executives across industry and business through various channels, starting with those organizations that played a role in its formulation and validation. Beyond this, relevant courses in business schools could be made available to this audience. It is key that this framework is seen as the starting point, and that it allows extension as the cybersecurity field evolves through new literature, and as the knowledge amongst Board Directors and Senior Executives grows. This mindset in its formulation is important so that it is not seen as a one-off outcome. The changing nature of the cybersecurity domain demands such agility and extensibility. In addition, each model in the framework could be the subject of further research to delve into more detail that can assist downstream stakeholders, including the CIO/CRO/CISO community, to better implement cybersecurity in accordance with the desired maturity.

1.5 Research Strategy

This research follows the design science research (DSR) method, across two linked phases: Development (Phase 1) and Evaluation (Phase 2), (Hevner & Chatterjee, 2010; Hevner et al., 2004). The DSR method enables a clear focus on output artefacts that assist in addressing the problem statement for Board Directors and Senior Executives. This also assists in framing the usefulness, quality, and applicability of the framework, and better enabling further research to build and extent these outputs. This approach is akin to that taken by (Manson, 2006) which posits that output artefacts that are grounded in rigour and assist to solve a specific problem are developed across two focus areas covering the ‘design’ and ‘evaluate’ phase. This two-phase approach is broken down further into four stages that are relevant to the research question. Figure 3 depicts the research strategy.

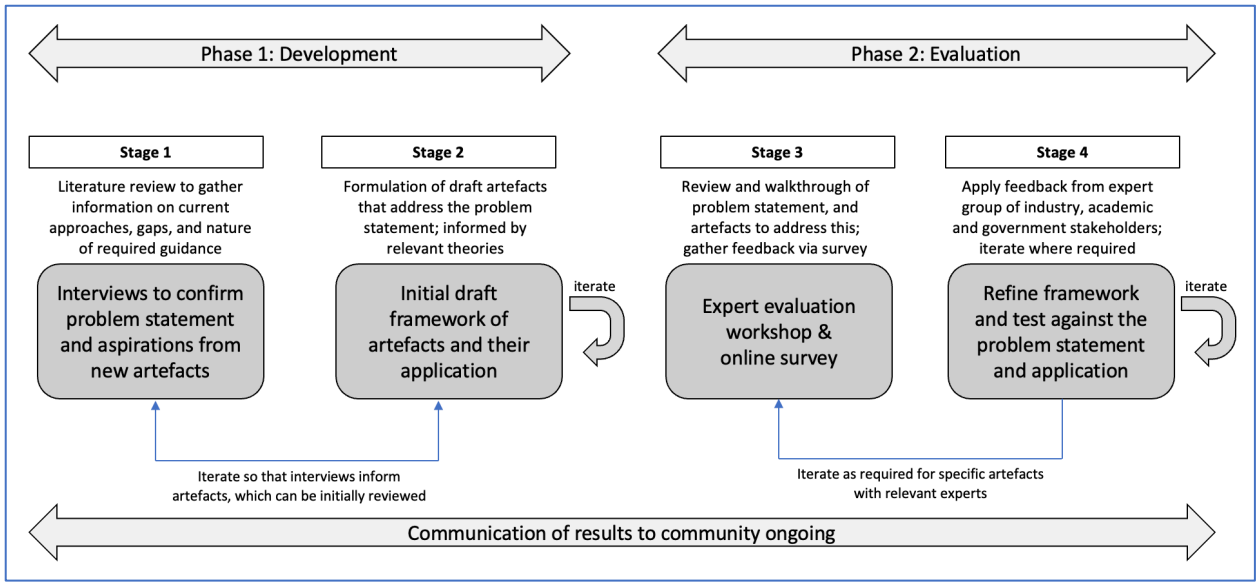

Figure 3: Research strategy

Phase 1 (Development) identifies the research problem and subsequently proposes an initial draft BCGF as a solution based on the literature review that examines the academic literature, industry and business papers/practices, and interviews with experienced NEDs, CIOs and CISOs. The 15 interviews were conducted through a qualitative approach to capture participant pain points and aspirations experienced when they were governing cybersecurity. Grounded theory (GT) techniques augmented the DSR to synthesise the concepts discussed in the interviews and confirm the needs that were unmet. This allowed the initial formulation of the framework and underpinning models with a sound basis of traceability to real-world industry/business challenges synthesised at the outset in the literature review.

Phase 2 (Evaluation) evaluates the draft framework via an Expert Evaluation Workshop (EEW) involving selected academics, NEDs, CIOS, CISOs and industry business SMEs. These consisted of the 15 interview participants, with additional subject matter experts, such as consulting partners and academic researchers, who provide cybersecurity advice to Boards and Senior Executives, for example, the Partner for Cybersecurity at Boston Consulting Group (BCG) and the Professor of Cybersecurity Research at MIT. A walkthrough of the framework was conducted, along with a discussion and feedback on the use of the framework in practice. An online Expert Evaluation Survey (EES) of 20 participants subsequently captured more detailed feedback on the proposed framework quantitively which then allowed refinement and improvement of the framework. Following on from this, various models of the framework were applied to specific Board discussions as depicted in the section List of Publications and Presentations. This helped in the further refinement of usage guidelines for the proposed BCGF.

1.6 Proposed Solution

The two-phase DSR approach was applied to develop and evaluate the BCGF that aims to assist NEDs and CXOs better govern cybersecurity. Figure 4, depicts the highest-level conceptual model of the BCGF; further detail is defined Chapter 5.

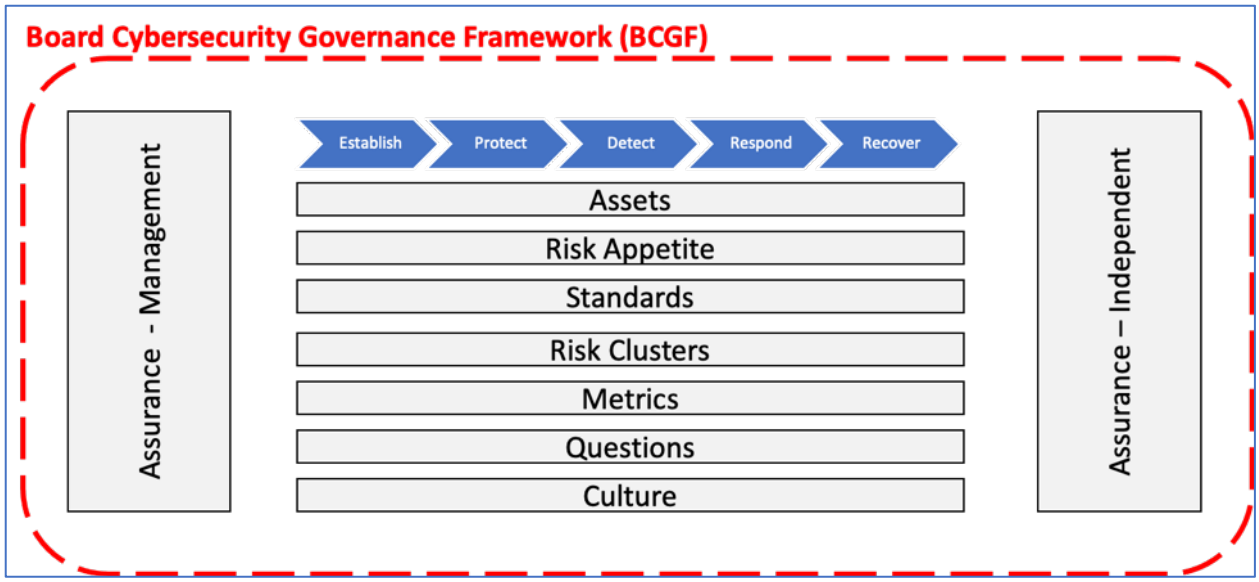

Figure 4: Board cybersecurity governance framework (BCGF) – level 1

Three core concepts are embedded in the BCGF; a *journey view* to depict the stages in the cybersecurity lifecycle, a *stakeholder view* to show the various actors, and a *perspective view* to depict their role in governance or implementation. The journey view is depicted in Figure 5. This shows a lifecycle approach to cybersecurity governance to enable a targeted approach to asking the right questions (at the right time), setting the tone, expectations of the risk appetite and the urgency of cybersecurity matters at the Board level. Whilst this lifecycle has the basis from NIST (NIST, 2018), this research refined this for a Board audience with more clarity of the aims and activities Board Directors should specifically be undertaking.

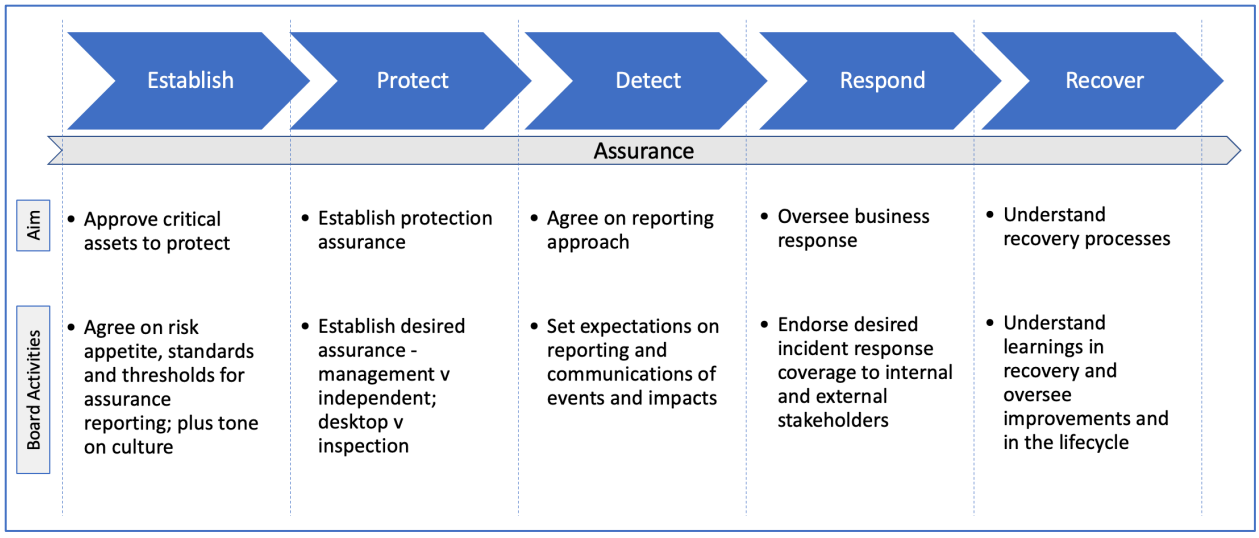

Figure 5: Stages in board cybersecurity governance

The linkage of the stages to stakeholders or actors is also key so that there is two-way alignment from the roles that govern cybersecurity to roles that implement cybersecurity. Figure 6 depicts the layers of stakeholders along with the *perspective* they have in terms of whether they govern and/or implement cybersecurity. The focus of the BCGF is on how NEDs/CXOs can govern better, given the gaps in literature and practice on 'how' they do this. It is anticipated that targeting this stakeholder group will assist enabling traceability to other stakeholders such as the CIO, CISO and various SMEs, who are responsible for implementation of cybersecurity controls, from an alignment perspective.

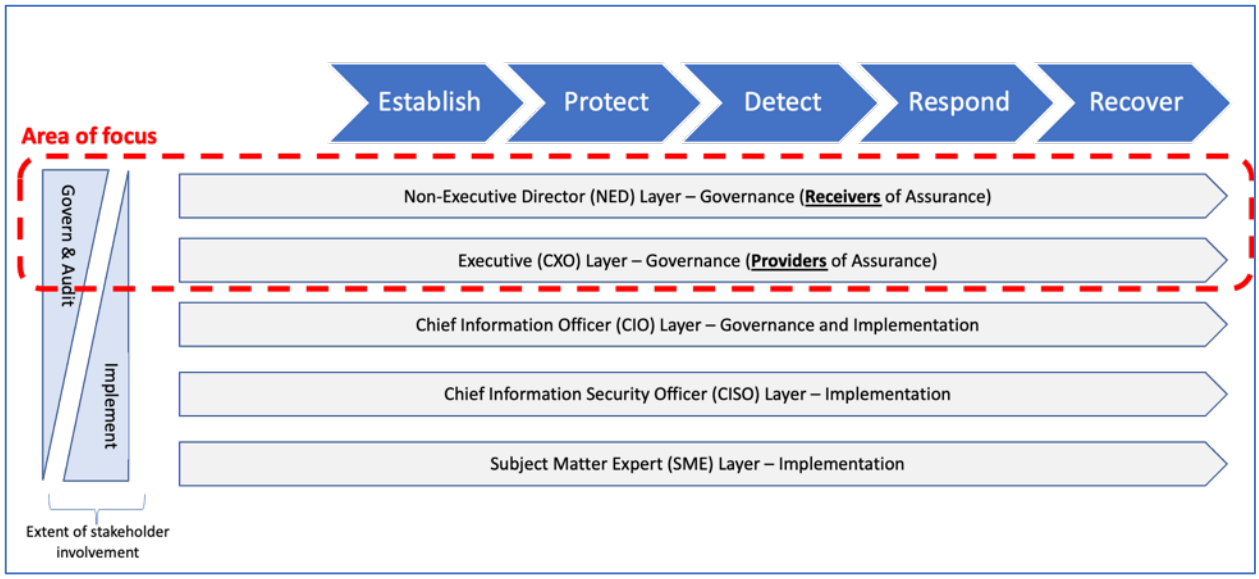

Figure 6: Focus of framework

The core part of the framework centres on 7 foundational models that sit inside the BCGF as depicted in Figure 7. These models were identified from the literature review, pain points and aspirations expressed by interviewee participants, and expert evaluation through the workshop and online survey. Further, the concerns expressed by NEDs/CXOs in the course of interviews informed the minimum set of models, which over time, could be evolved and improved upon. Participants expressed the need for flexibility in the BCGF to aid a fit-for-purpose approach in its application. As such, each of the models is standalone which allows the BCGF to be applied in whole or part, depending on the needs and maturity of the relevant organization. As a collective, the models address the needs for Board cybersecurity governance, as demonstrated in Chapter 6 - Results and Evaluation. Given the evolving nature of cybersecurity models, it is expected that insights will be gleaned from further application and research.

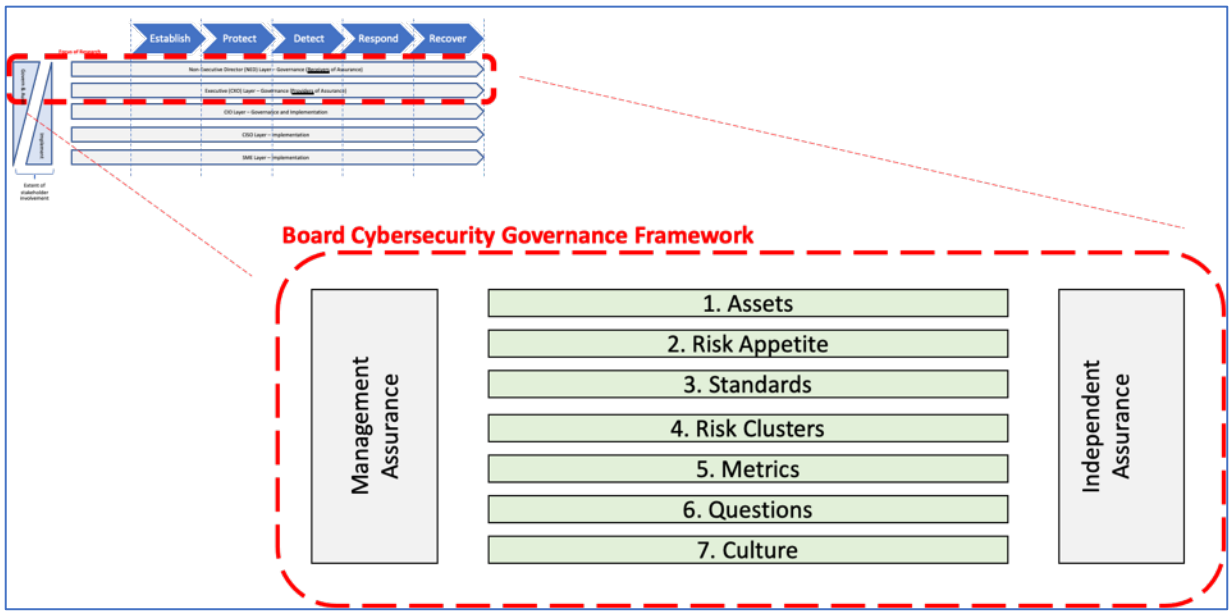

Figure 7: Context of BCGF

The 7 foundational models, including their aim and their applicable business scenario are outlined in Table 2. These are further discussed in detail in Chapter 5.

Model #	Model Name	Aim of Model	Applicable Business Scenario
1	Assets	Determination of the assets (commonly referred to as the 'crown-jewels') that warrant specific protection from cybersecurity risks.	Establish risk appetite statement, compliance & assurance reporting
2	Risk Appetite	Outline the acceptable impact or consequences from a cybersecurity incident specifically to the assets determined as the 'crown-jewels'.	Establish risk appetite statement
3	Standards	Identify standards against which the organization will measure its effectiveness against. Includes evolution towards other standards of relevance.	Establish risk appetite statement, compliance & assurance reporting
4	Risk Clusters	Identify of cybersecurity risk themes bases in internal and external factors, to then shape the education and program of work.	Board education, risk management, industry trends
5	Metrics	Ensure the right metrics are identified to track the quality of cybersecurity.	Compliance & assurance reporting
6	Questions	Frame questions to probe and understand the cybersecurity landscape and understand the scope and depth of the desired assurance.	Board & sub-committee meetings
7	Culture	Determine the desired and actual cybersecurity culture, and metrics that can be lead indicators in understanding this.	Compliance & assurance reporting, board & sub-committee meetings

Table 2: Models in BCGF and their aim

1.7 Application and Users

The proposed BCGF is intended to be used mainly by Board Directors and Senior Executives pursuing Board-level cybersecurity governance. However, other stakeholders, such as CIOs, CISOs, CROs, auditors and regulators may also glean value from this to understand the approach to cybersecurity governance being established by their Board of Directors. The framework can be used by stakeholders to help fulfil their cybersecurity governance accountabilities in the private or public sector. This can be in setting the strategy and tone of the intent from a senior governing body such as a Board for management to follow and implement. It is expected that the framework will involve context-specific tailoring and extensions for different industry sectors as per governance, regulatory and compliance requirements relevant to their areas of operations. The BCGF is not limited to application in any specific sector. Research included experts from cross-industry, government and academia. However, use of this will require tailoring to make it fit-for purpose across various sectors. It is important to note that cybersecurity governance is a global issue, and this research, while conducted in Australia, may have broader applications and use subject to further research. Hence, there is no reason why applications and users should be limited to Australia. Furthermore, this research includes input from interview participants and experts who have work experience in international markets from directorships, executive roles, consulting services and academic research. This provides a broader international perspective into the evaluation of the BCGF to improve its contribution.

1.8 Structure of Thesis

This thesis is organised into 7 Chapters as detailed in Table 3.

Chapter	Title	Coverage
1.	Introduction	Overview of the problem, literature review, research method and the solution.
2.	Research Background and Problem	Background context and the business challenges currently facing industry that have led to the problem.
3.	Literature Review	Prior research and significant industry and business papers that are related to the problem statement.
4.	Research Method	The research strategy and steps to formulating the solution and then validating it.

Chapter	Title	Coverage
5.	Board Cybersecurity Governance Framework (BCGF)	Detail of the solution framework developed through this research, including the various models.
6.	Results and Evaluation	Construction and evaluation of the BCGF developed through the stated research method.
7.	Discussion and Conclusion	Analysis of the use of the framework, its application, future research in this area, and its use in industry.

Table 3: Structure of thesis

1.9 Summary

Cybersecurity governance at the Board level is a complex undertaking given the challenges introduced through a dynamic threat landscape, emerging new regulations and reporting, changing technology solutions and risks. There is a lack of research-based practical framework that may assist Board Directors and Senior Executives to achieve their cybersecurity governance aims and activities. To address this problem of Board-level cybersecurity governance, a research-based BCGF has been developed and evaluated using the well-known DSR research approach (and augmented with grounded theory techniques). This framework consists of 7 foundational models that aim to assist Board Directors in governing the posture of cybersecurity and as well as being a guide for Senior Executives when they are providing assurance on the posture of cybersecurity in their organizations. The framework will help such stakeholders better articulate the intent in cybersecurity strategy and allow improved alignment to the various roles that implement these requirements. Further research and extension of the framework is required in an ongoing manner due to the changing nature of cybersecurity. This chapter provided an overview of the research problem and proposed solution including the adopted research strategy. The remainder of this thesis will further detail the topics introduced in this chapter. The next chapter will provide a detailed account of research background and problem that has been systematically identified and addressed in this research.

2 Research Background and Problem

2.1 Introduction

The previous chapter provided an overview of this research, including the introduction to the research problem, and the overall research strategy to formulate the proposed solution. This chapter delves into the research background and problem statement, as well as covers conceptual foundations, cybersecurity implementation methods currently being used, and elements of cybersecurity governance at a Board level. It then details the research question, aims, objectives, and deliverables of this research.

2.2 Conceptual Foundations

The term cybersecurity is used in various contexts and often has a different meaning to researchers and practitioners who need to interpret it as appropriate to their work. If we examine dictionary sources, academic literature, and industry/business practices, we can arrive at a common understanding of the definition. Cybersecurity as a term only stems from 1995 onwards, with the broader adoption of the public internet and a growth of commercial online services that drew the attention of criminals. By way of example, internet banking capability was launched by a number of Australian banks from the late 1990s. The existing literature (Warner, 2012) also reinforces the relatively recent definition of this term but argues that the concepts of cybersecurity existed from the late 1960s under the guise of 'information security'. This argument revolves around the evolution of computers from standalone machines in the 1960s that held sensitive data and therefore required protection with what were largely physical controls. Then, in the 1970s, as interconnected networks grew, data theft and attacks on systems became more common, requiring additional information security controls in systems, including more sophisticated authentication and authorisation mechanisms. There is no universally accepted single definition of the term 'cybersecurity' and we must examine a number of definitions to synthesise a common definition for the purposes of this research. The sources of definitions include dictionaries and academic and industry/business sources as shown in Figure 8. Definitions from each of these sources are now covered.

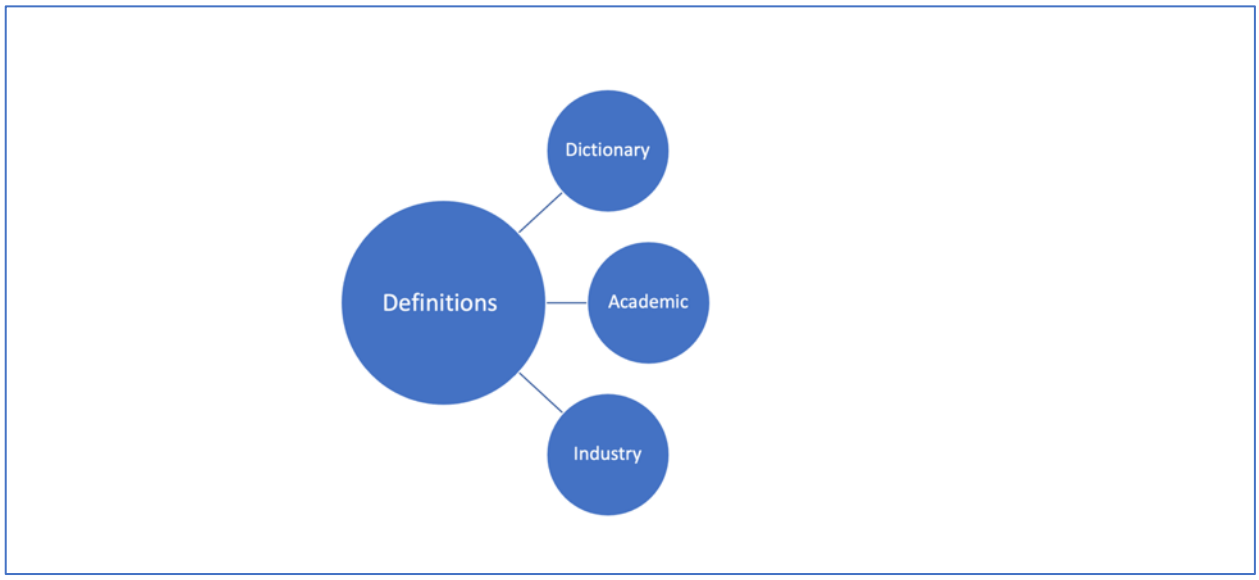

Figure 8: Cybersecurity definition sources

2.2.1 Dictionary Definition

When looking at English language dictionary sources, a common approach is to state cybersecurity as being the act of protecting data belonging to individuals and organizations from criminal or unauthorised systems access. The Oxford dictionary (Stevenson, 2010) refers to this "as the state of

being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this", whereas the Meriam-Webster dictionary defines this as the "measures taken to protect a computer or computer system (as on the Internet) against unauthorised access or attack" (Merriam, 2013). The (*Cambridge English Dictionary*; Press, 2011) takes a similar view and defines this as "things that are done to protect a person, organization, or country and their computer information against crime or attacks carried out using the internet". When examining the definition from various dictionary sources, one aspect worthy of note is that there is no qualifier to the way protection is established. In other words, definitions do not limit protection to controls with people, processes, or technology. Definitions are inclusive of all dimensions and could include things like 'culture' and 'awareness'. This makes the cyber security field very broad and prone to being interpreted widely. The major dictionary definitions along with the key concepts represented in each definition are shown in Table 4.

Definition	**Key Concepts**	**Reference**
The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.	Authorization, protection measures, electronic data	Oxford (Stevenson, 2010)
Measures taken to protect a computer or computer system (as on the Internet) against unauthorised access or attack.	Authorization, protection measures, computer system	Webster (Merriam, 2013)
Things that are done to protect a person, organization, or country and their computer information against crime or attacks carried out using the internet.	Protection measures, computer system, network, awareness	(*Cambridge English Dictionary*; Press, 2011)
The state of being safe from electronic crime and the measures taken to achieve this	Protection measures, electronic crime, electronic data, culture	Collins (Wilkes & Krebs, 1995)
Protection provided for an information system, such as computer and telecommunications networks, against cyberthreats.	Protection measures, computer system, network	Macquarie (Butler, 2017)

Table 4: Dictionary definitions of cybersecurity

2.2.2 Academic Definition

Whilst academic literature has taken a more precise view of the definition, there remains some level of variability. In many cases, authors have stated their assumed definition upfront in papers to avoid ambiguity (Azmi et al., 2018), whilst (Craigen et al., 2014) argue the case that definitions are highly variable and that the multidimensions of cybersecurity are not captured in any existing definition. The authors propose that cybersecurity is "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." The aim of this definition is to intentionally have a broad scope given the multidimensional nature of cybersecurity. The use of a "collection of resources, processes and structures" is a catch all to include interactions of humans and systems, as well as other (yet to be defined) concepts. Whilst this makes the definition broad, it is also therefore adaptive and dynamic, as newer technologies and threats evolve in this field. The Software Engineering Institute (Cebula et al., 2014) breaks down cybersecurity into a taxonomy of four dimensions. This includes, actions of people, systems failures, process failures, and external events. This brings a more defined scope, however aspects related to people and their behaviour are only covered lightly under failed internal processes, (under the category of supporting processes on staffing and training). Further, (Azmi et al., 2018) report the issue of a non-standard definition and propose the following definition for their work on cybersecurity frameworks: "securing a virtual digital environment by governance, management and assurance, including its assets (i.e. information assets and cyber assets), entities (such as end users, organizations, governments, societies, machines and software), and interactions (enabled by IT infrastructure, communications/networks, systems and devices". Another aspect of the definition of cybersecurity is the concept of 'information security'. This has also been a topic of discussion given the strong relationships between these. This relationship is described by (von Solms & van Niekerk, 2013)

who argue that whilst there is a substantial overlap of concepts, the two are not completely analogous. They argue that cybersecurity also considers, amongst others, aspects that are related to the human elements associated with attackers and victims. A related set of definitions has been identified through a review of three well-known databases and are summarised in Table 5. The three databases include, ("IEEE Xplore," 2000), ("Scopus," 2008), and ("ScienceDirect," 2021). These are chosen as representative of the majority of academic views across the literature in scope.

Definition	Key Concepts	Reference
Securing a virtual digital environment by governance, management, and assurance, including its assets (i.e. information assets and cyber assets), entities (such as end users, organizations, governments, societies, machines, and software), and interactions (enabled by IT infrastructure, communications/networks, systems, and devices).	Digital environment, assets, entities, devices, awareness	(Azmi et al., 2018)
Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.	Cyberspace systems, protection measures, resources, processes	(Craigen et al., 2014)
Cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders.	Detect, defence, Intruders	(Kemmerer, 2003)
Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets.	Resources, protection measures, digital environment, assets	(ITU, 2008)
The art of ensuring the existence and continuity of the Information Society of a nation, guaranteeing, and protecting, in Cyberspace, its information assets and critical infrastructure.	Continuity, protection measures, information assets	(Canongia & Mandarino, 2012)
The protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal, and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace	Electronic information, cyberspace users, vulnerability	(von Solms & van Niekerk, 2013)

Table 5: Academic definitions of cybersecurity

2.2.3 Industry Definition

While this research is applied in nature, common industry definitions in recent years have been included to compliment the academic definitions. Industry largely refers to the people aspects along the well-known triad of confidentiality, integrity, and availability of the data. For example, the Cybersecurity & Infrastructure Security Agency (CISA, 2019) and (CISCO, 2021) define cybersecurity as the “practice of protecting systems, networks, and programs from digital attacks.” The Information Systems Audit and Control Association (ISACA) recognised the variability of the definition and aimed to converge different perspectives. (Rout, 2015) details the industry challenges that commence from even being unable to agree upon whether its ‘cybersecurity’ (one word) or ‘cyber security’ (two words), and then the semantics of the relationship to ‘information security’ coming into play. The information security term was clearly adopted in the mid-1900s, and over the years since, the use of cyber has become more prominent in industry. (NIST, 2019) in its glossary of terms defines cybersecurity as the ability to protect or defend the use of cyberspace from cyber-attacks where cyberspace is defined as a global domain of networked systems. Whilst simplistic and technical in nature, this does leave the full scope to the reader, whether the ‘ability’ is technical, non-technical or some other dimension. The lack of a single definition of cybersecurity plays out in industry practices, where very often seen in internal and external company audit plans are separate overlapping audits in the form ‘information security’ and ‘cybersecurity’. When questioning the basis for this separation, there is no logical explanation in many cases, which is reflective of the lack of an agreed academic definition. Technology research company

Gartner (Walls et al., 2014, p. 2) also confirms this confusion and offered a definition that is grounded in military terminology, by saying cybersecurity is "the governance, development, management and use of information security, operational technology security, and IT security tools and techniques for achieving regulatory compliance, defending assets and compromising the assets of adversaries". Gartner also posits that cybersecurity is a superset of elements like information security, operational technology security, and security practices for digital assets. This is very much in line with the assertions of (von Solms & van Niekerk, 2013) who indicate there are elements of cybersecurity that sit outside of information security. Interestingly, (Taherdoost, 2022) argues the complete opposite and views information security as being the superset within which cybersecurity exists. The Cyber Security Body of Knowledge (CYBOK) takes the position, by virtue of its approach of being a body of knowledge, of providing references to other definitions, rather than introducing its own (CyBOK, 2021). A summary of industry definitions of cybersecurity across regulations, standards and practices is presented in Table 6.

Type	Definition	Key Concepts	Reference
Regulation	Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.	Authorization, protection measures, confidentiality, integrity, availability	CIS Agency (CISA, 2019)
Regulation	The preservation of an information asset's confidentiality, integrity, and availability. (Note the standard uses the term information security to include cybersecurity).	Information security, confidentiality, integrity, availability	(APRA, 2019)
Standard	The ability to protect or defend the use of cyberspace from cyber-attacks.	Protection	(NIST, 2019)
Standard	Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets.	Tools, policies, protection measures, assets	(ITU, 2008)
Industry / Business Practice	Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.	Protection measures, systems, networks	(CISCO, 2021)
Industry / Business Practice	Cybersecurity is the governance, development, management and use of information security, OT security, and IT security tools and techniques for achieving regulatory compliance, defending assets, and compromising the assets of adversaries	Governance, tools, techniques, compliance, assets, defend, compromise, adversaries, awareness	Gartner (Walls et al., 2014)

Table 6: Industry definitions of cybersecurity

2.2.4 Synthesis

An examination of the definitions of cybersecurity across dictionary, academic and industry/business sources reveal there is not one agreed definition of cybersecurity. Hence, for NEDs and CXOs, discharging their cybersecurity governance responsibility becomes even more difficult due to the lack of an agreed definition, in what is already a complex and ever-changing topic. In fact, (Cains et al., 2021, p. 25) argue that current definitions are "inadequate due to lack of inclusion of human factors, no standardized cyber security terminology exists across disciplines". However, there is a convergence in views, whereby cybersecurity is seen as not merely being limited to the domain of the technology or the processes required to maintain it. It also encompasses other aspects, such as human behaviour and culture (Cebula et al., 2014). It is often seen as associated with the way people compromise systems for data theft and intelligence, and the required protection mechanisms to prevent this. An example of this is social engineering to compromise systems, which may be minimised through a focus on security culture and awareness. The concepts found in the various cybersecurity definitions examined are

synthesised in Figure 9. As can be seen, the many facets of cybersecurity make it very difficult to define due to the breadth and depth it covers.

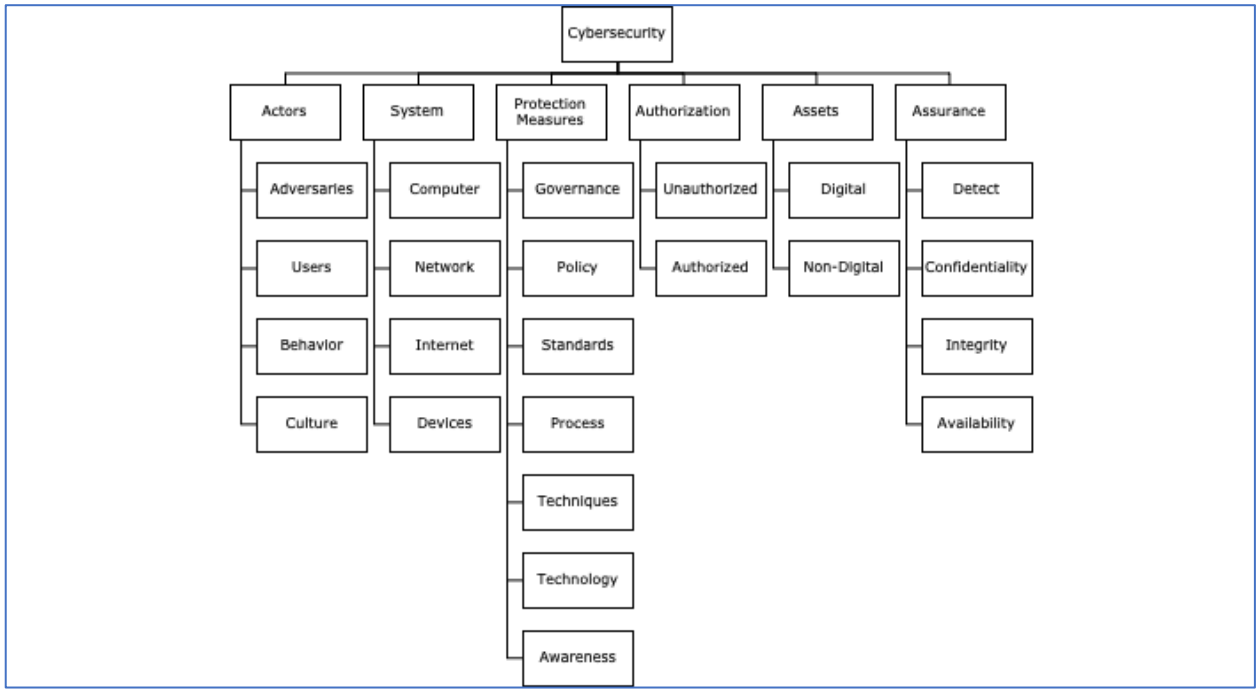

Figure 9: Concepts in cybersecurity definitions

However, for the purposes and scope of this research, the following definition is assumed, namely cybersecurity is "the protection of technology systems from unauthorized access through a range of protection measures covering people, processes and technology, that safeguard the confidentiality, integrity and availability of the systems themselves, and information held within them". This enables the inclusion of soft elements, such as people, culture, and behaviour (dealing with the social engineering threat), along with hard elements such as policy, standards, and technology (dealing with the technical aspects in systems).

2.3 Cybersecurity Implementation

Arriving at a definition of cybersecurity provides initial conceptualisation; however, its implementation requires concrete methods. The method or approach to implement cybersecurity entails selecting an appropriate standard or overarching framework and then formulating a program of works to progress towards this. It is this approach that is defined by Shackelford et al. (2015) which has its basis in the adoption and implementation of a cybersecurity framework (which in many cases us also referred to as a cybersecurity standard). In this context, a cybersecurity framework is defined as a set of processes, informed by specific standards and guidelines, that are representative of best practice to improve the cybersecurity posture in an organization. Further, the use of an industry-wide framework can be a way to reduce implementation costs and help protect critical systems in a more informed and structured manner (Kosutic & Pigni, 2021). The lack of a common cybersecurity definition has manifested downstream into cybersecurity implementations where there are number of generic frameworks and standards to choose from, along with unique ones that are local to certain geographies or specific to an industry sector. The literature has extensively identified and analysed the popular implementation methods available at an international, local and industry-specific level (Dedeke & Masterson, 2019; Donaldson et al., 2015; Shackelford et al., 2015; Shariffuddin & Mohamed, 2020; Smith et al., 2019). A summary of the core implementation methods is shown in Table 7.

Method #	Framework	Geography	Sector	Reference(s)
M#1	ACSC Essential 8 (E8)	Australia	Generic	(ASD, 2020)

Method #	Framework	Geography	Sector	Reference(s)
M#2	ACSC ISM	Australia	Government	(ASD, 2023)
M#3	COBIT 5	International	Generic	(Harmer, 2013)
M#4	ISO/IEC 27000/01	International	Generic	(ISO, 2013a, 2013b)
M#5	PCI DSS	International	Payments	(PCI, 2018b)
M#6	NIST	International/USA	Generic	(NIST, 2019)
M#7	CIS 18	International/USA	Generic	(CIS, 2021)
M#8	Cyber Essentials	UK	Generic	(GCHQ, 2023)
M#9	FISMA	USA	Generic	(FISMA, 2014)
M#10	SOC 2	USA	Generic	(AICPA, 2022)
M#11	AESCS	Australia	Energy Sector	(AEMO, 2019, 2023)

Table 7: Common cybersecurity implementation frameworks

When examining these frameworks and standards in more detail in Table 8, it becomes clear that the focus on NED and CXO stakeholders is limited, and the scope is primarily directed at the cybersecurity technical professional or subject matter expert charged with cybersecurity implementation and operationalisation. This presents a challenge in that there is a lack of guidance to the NED and CXO audience on which framework their organization should be implementing, and the contents of the various frameworks do not assist this stakeholder group in explaining the nuances of the implementation in the right business language.

Method #	**Audience**	Lifecycle approach	Roles & Responsibilities	Threats	Policy	Risk/Program Management	Security Planning	Personnel / Users	Assurance	Personnel / Users	Contingencies & Disasters	Incident Handling	Awareness & Communications	Operational Controls	Physical Security	Identification & Authentication	Access Control	Audit Trails	Cryptography
M#1. (E8)	NED/CIO/CISO			√	√	√		√	√					√		√	√		
M#2. (ISM)	CIO/CISO		√		√			√		√		√		√	√		√	√	√
M#3. (COBIT)	CIO/CISO	√	√			√	√						√						
M#4. (ISO)	CISO		√		√	√	√	√	√	√		√	√	√	√	√		√	
M#5. (PCI)	CISO																		
M#6. (NIST)	NED/CIO/CISO	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
M#7. (CIS)	CISO			√	√	√		√	√					√		√	√	√	
M#8. (Cyber Essentials)	CIO/CISO		√	√	√	√				√		√	√			√		√	
M#9. (FISMA)	CIO/CISO	√	√		√	√	√	√	√			√	√	√		√	√	√	
M#10. (SOC2)	CIO		√		√	√			√					√	√	√	√	√	
M#11 (AESCS)	CIO/CISO			√	√	√		√	√	√		√		√		√	√		

Table 8: Coverage of cyber implementation methods against NIST concepts

In terms of general applicability at an industry level, NIST provides a comprehensive baseline end to end, and has been seen in industry as having an all-inclusive scope on which an organization should focus for good cybersecurity measures. NIST has been used as the baseline in Table 8 to compare the breadth of other commonly used implementation methods. It provides introductory sections and a lifecycle approach that is very applicable for the NED/CXO audience. However, beyond this initial content, NIST delves very quickly into technical aspects for the CIO/CISO audience.

Following on from the analysis of cybersecurity implementation methods, this leads into the area of cybersecurity governance in terms of the extent to which NEDs and CXOs can use these to better provide oversight and assurance on the posture of cybersecurity in their organization.

2.4 Cybersecurity Governance

Following on from the definition of cybersecurity and cybersecurity implementation methods, it becomes important to understand how cybersecurity is governed in terms of overseeing and directing investments and resources towards the desired maturity. This oversight, or 'governance' has been explained as "setting clear expectations for the conduct (behaviours and actions) of the entity being governed, and directing, controlling and strongly influencing the entity to achieve these expectations"(Allen, 2005, p. 10). In the context of Board cybersecurity governance, this is often stated as the activities to align the maturity of cybersecurity (and sustain this) to the desired thresholds to support the business goals and strategies (AlGhamdi et al., 2020). There are several facets in governance, including setting policy, authority, control, influencing and regulating the entity in question. For the purposes of Board cybersecurity governance, three foundational elements are relevant, as shown in Figure 10. These are the *oversight* required to ensure the right cybersecurity maturity, the *frameworks* that can be used to apply this authority, and finally the *compliance* elements necessary in a regulated environment such as financial services. These three elements represent a synthesis of the concepts identified in (AICD, 2022a).

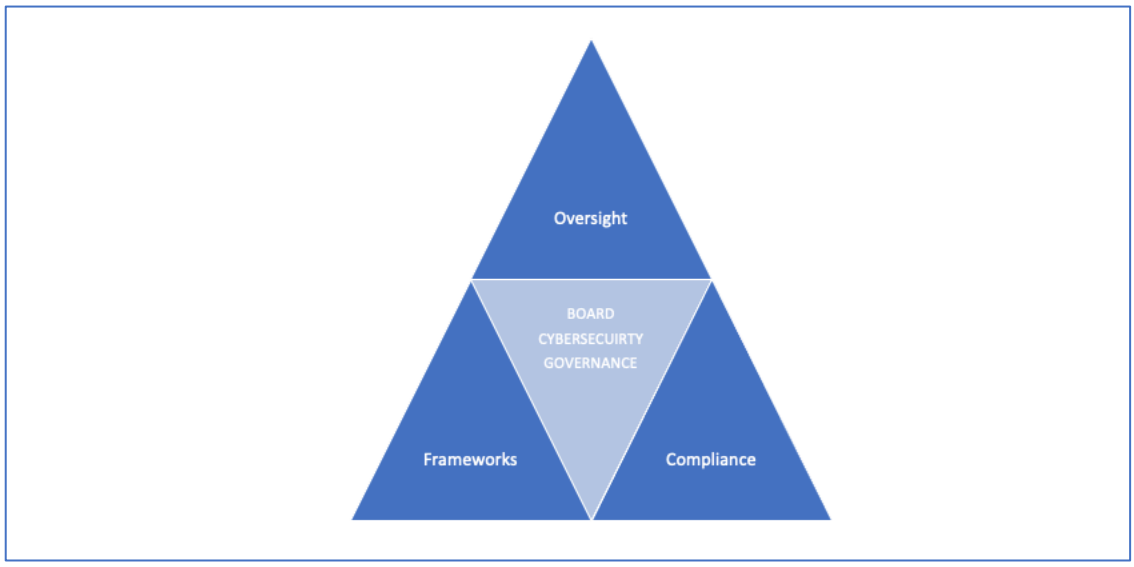

Figure 10: Elements of board cybersecurity governance

2.4.1 Oversight

Cybersecurity oversight begins at the Board level with the setting of the business strategy and goals and defining and embedding a risk framework to guide delivery. Whilst a two-way discussion naturally occurs with management, the approval and setting the tone of the strategy remains with the Board. For government entities, this follows a similar approach, with relevant local, state, and federal ministerial teams driving the plans. The cybersecurity agenda is an inherent part of this process in mature organizations so that it is part of the strategic and risk roadmap and is aligned to the organizational goals and intent. It is interesting to note however, whilst this alignment of cybersecurity to business goals is cited as essential in many sources, such literature falls short in identifying consistent metrics, thresholds and terminology that may be appropriate to measure the maturity or extent of alignment from an executive or Board standpoint. Whilst AlGhamdi et al. (2020) and also Bruin and Solms (2016) report the need for top-level management and Board-level focus to drive maturity, they fall short of providing specific dimensions or frameworks to track and report upon. When coupled with varying definitions and explanations of cybersecurity and information security, this makes it particularly difficult for senior leaders who govern organizations to comprehend the true state of risk in their operations.

Regulators also have, in recent years, included specific requirements for Boards, with APRA (2019, p. 7) directing in its CPS234 standard that "the Board of an APRA-regulated entity is ultimately responsible for the information security of the entity. The Board must ensure that the entity maintains information security in a manner commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity." In practice, this accountability has limited support in the way of business-level frameworks and models that can be used to fulfil this accountability with ease. Regulated entities are having to infer their own specific mechanisms to provide this assurance. This issue is compounded as the scope of regulations has increased to organizations providing downstream assurances on their suppliers, each of which has a different way of reporting and measuring their own cybersecurity posture.

2.4.2 Frameworks

As the importance of cybersecurity governance has become more critical for organizations, a number of frameworks have evolved to guide the implementation of processes and controls. These stem from the literature related to IT governance, with extensions added for cybersecurity risk. The Information Security Governance and Management (ISGM) framework from Carcary et al. (2016) has its basis in COBIT as outlined by Harmer (2013) and the Open Group (OpenGroup, 2017). Similarly, security standards from ISO, such as ISO (2018), (ISO, 2013a) and (ISO, 2013b) have detailed key processes and controls expected in organizations. Whilst these frameworks are comprehensive and drive a greater focus on strengthening security, they are focussed on security or risk practitioners and have an inherent level of assumed knowledge in this domain. A number of industry-specific frameworks that delve more deeply into the issues faced by organizations in specific sectors have also been released. The energy sector is one case in point with the Australian Energy Market Operator publishing (AEMO, 2019). This has its basis in ISO/IEC and NIST standards and focuses on the maturity of key processes that must be in place for sound cybersecurity management (NIST, 2018). These include aspects such as asset, change and configuration management, identity and access management, and event/incident response, including business continuity. The audience for this framework again is risk and security practitioners. In addition to frameworks, organizations have also focussed on strengthening the professional expertise and technical capability of practitioners. This has been through driving a focus on the accreditation of people in qualifications such as Certified Information Management Security Manager (CISM) from ISACA (2022), and Certified Information Systems Security Professional (CISSP) from ISC2 (2024). In part, this has been driven by the need to uplift capability, but also there has been a need to broaden the knowledge across a larger group of people due to the scarcity of expertise in the cybersecurity field. Specifically, this focus has helped to strengthen and grow skills in cybersecurity on an international basis for technical managers and security engineers/designers (Furnell et al., 2017).

2.4.3 Compliance

Regulated entities have faced increasing scrutiny on the posture of their cybersecurity given the impact on the organisation and the broader economy from a breach of security. This is not limited to financial services, which has historically been heavily regulated on operational risk matters for many years. By way of example, the Australian Securities and Investment Commission (ASIC) has published a range of standards for companies on good cyber resilience, including (ASIC, 2015). It has, over time, increased its oversight of the corporate sector to highlight good practices and areas in which to improve (ASIC, 2019). Furthermore, the ASX also conducted a health check of the ASX 100 companies and published its findings in (ASX/ASIC, 2017). This report concluded with findings that are also very reflective of themes across other organizations in Australia and the key insights and metrics are shown in Table 9.

Insights	Metrics
Cybersecurity is a major and growing risk	Only 34% of Boards have a clearly defined cyber risk appetite
Tackling cyber risk needs a culture of collaboration (amongst organizations)	Only 50% of Boards are somewhat confident that their company is properly secured against cyber-attacks (43% appear confident)

Insights	Metrics
Boards take cyber risk seriously and are improving their skills	Only 11% of Boards have a clear understanding of where the company's key information and data assets are shared with third parties
Companies are managing cyber risk better but realise there's still more to do	Only 32% of companies access their cyber culture annually

Table 9: Insights and key metrics from (ASX/ASIC, 2017)

It can be observed from the aforementioned insights that only 11% of Boards have a clear grasp of their environment subject to cybersecurity. These insights and metrics clearly show there is much more to be done to increase the knowledge and awareness of those in senior leadership who are directing or governing organizations. This marks the need for further work and strong motivation for the research reported in this thesis. Further, it should be noted that regulators are now increasingly initiating criminal charges against organizations that demonstrate poor practices in cybersecurity such as (APRA, 2023; ASIC, 2020). Such developments and directions clearly raise the importance of good cybersecurity governance in industry and business. This focus is also apparent in specific industries where existing industry standards have been extended to address the needs of that sector. This includes financial services regulators, such as the Australian Prudential Regulation Authority (APRA, 2019), and industry bodies such as the Payment Card Industry PCI (2018a) which prescribes specific controls and governance over card-related data. Further, governments have also focussed their attention on the utilities sector (power, electricity, gas, water, etc.) which fall into the category of critical infrastructure protection for systems of national significance (AEMO, 2019).

2.4.4 Synthesis

There are many documents that are involved in governing the cybersecurity posture of organizations, with examples being strategies, policies, guidelines, processes, and standards. For the purpose of this research, these are generically termed cybersecurity artefacts. These cybersecurity artefacts begin with general government guidance such as that from Australian Cyber Security Centre (ACSC, 2021), and industry bodies such as the Australian Cybersecurity Growth Network (AustCyber, 2021). More detail is then present in ISM/ISO/NIST standards from international bodies. Some industries have extended these standards to their own specific versions in order to stress key elements as appropriate to their local context. A key challenge in having so many cybersecurity artefacts is to ensure standards are fit for purpose for the relevant organization. This requires understanding the benefits and cost of compliance while balancing the end user experience and operational viability. Furthermore, appropriate mechanisms need to be embedded to understand and manage the implementation to the desired state.

2.5 Research Background and Related Work

A range of challenges for NEDs and CXOs have been observed from the literature analysis spanning cybersecurity and cybersecurity governance. It is evident from the analysis that there is a lack of a research-based framework and guidance for cybersecurity governance at the Board level. Furthermore, the current landscape is characterised by the following several dimensions that further compound this challenge.

- Cybersecurity standards exist in large numbers, and the difficulty often is in deciding which one to use as a baseline target for the nature and state of the organization;
- In most cases, the audience for standards is not the NED or CXO who ultimately govern/lead organizations, and standards require an intricate understanding of cybersecurity detail;
- A lack of guidance through models on how to establish the right mix of business-level metrics that can give assurance on the posture of cybersecurity;
- The terms framework, standard, and mitigation strategies are used interchangeable in industry and no agreed view on the terminology, akin to the cybersecurity definition covered in section 2.2 Conceptual Foundations.

For the NED and CXO stakeholders, these challenges pose several difficulties given the inherent technical nature of the cybersecurity field. These challenges are now covered in further detail.

2.5.1 Cybersecurity standards

There are many technology standards to guide the maturity of cybersecurity with several similarities across them. There is no right and wrong when it comes to these, as most are targeted at reducing risk in a specific dimension. The selection of these depends on a range of factors, which includes the current maturity of the organization, and specific operational processes that may demand increased compliance or assurance. The Financial Services sector has been the leader in mitigating cybersecurity risk due to the specific attention regulators have given this sector with ASIC (2022, p. 1) stating that "cybersecurity is vital to all organisations operating in the digital economy, and nowhere is this more important than the financial markets sector". As such, given this focus and by way of an example, Table 10 outlines the many standards that are relevant for the financial services sector in Australia.

Standard	Main Aim	Mandatory for regulated entity?	Reference
APRA CPS234	Improve Board governance of cybersecurity risk	Y	(APRA, 2019)
APRA CPS231	Address Outsourcing risk, including elements of cybersecurity	Y	(APRA, 2010)
PCI DSS	Mandatory requirements for collection, storage, and transmission of (cards) payment data	Y (if processing card data)	(PCI, 2018a)
SWIFT CSCF	Mandatory and advisory security controls for participants in the SWIFT payments network	Y (if using SWIFT network)	(SWIFT, 2020)
ISO/SEC 27001	Guide formulation of an information security system	N	(ISO, 2013a)
ISO/SEC 27002	Guide formulation of controls in information security	N	(ISO, 2013b)
ASD Essential Eight	A prioritised list of mitigation strategies to assist organizations in protecting their systems against a range of adversaries.	N	(ASD, 2020)
NIST Cyber Framework	Detailed technical controls to protect systems from cyber-attacks.	N	(NIST, 2019)

Table 10: Cybersecurity standards for financial services (Australia)

One can see some of these as foundational, such as CPS234 and CPS231, which are mandatory for entities regulated by the Australian Prudential Regulatory Authority (APRA). However, beyond this, the challenge in governance lies in choosing the appropriate baseline standard and then managing this. This becomes more difficult for NEDs and CXOs, who are held accountable from a legal perspective for having the appropriate security in their organization. This dilemma is visually demonstrated in terms of breadth and depth for each standard shown in Figure 11. This is very relevant as assurance becomes harder when the baseline can vary across organizations, and it can be more complicated in large organizations where each division may require some variability.

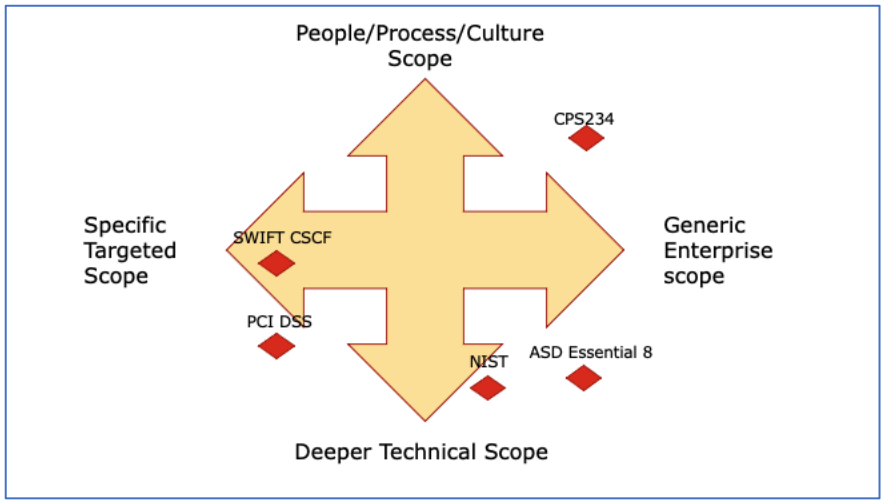

Figure 11: Facets of cybersecurity standards

2.5.2 Target Audience

The inventory of standards, frameworks, guidelines, and controls is large, and almost overwhelming for individuals who interact with the cybersecurity field. Interestingly, in examining a range of such artefacts, the SME in operational risk and cybersecurity is served well in terms of guidance and being the prime audience for these. The solution design and build teams are also well served in this regard. Table 11 has been produced through an examination of the level of detail in each artefact, the skills and experience required to comprehend this, and the stated intent of the artefact. Ironically the very user group (NED/CXO) that is now being held accountable for setting the direction and governing the cybersecurity risk profile, is the one that is served least in these artefacts.

Artefact[2]	**Primary Target Audience**						
	NED	CXO	Op Risk SME	Cyber Risk SME	Solution Architect	Software Designer	Software Developer
COBIT			√	√			
NIST			√	√	√	√	√
ISO/IEC 27000		√	√	√	√		
ISO/IEC 27001			√	√	√		
ISO/IEC 27002			√	√	√	√	√
CPS234 (APRA)	√	√	√	√	√		
CPS231 (APRA)		√	√	√	√		
CISM			√	√	√	√	√
CISSP				√	√	√	√

Table 11: Primary target audience for cybersecurity artefacts

When examining the literature on cybersecurity governance, there is limited knowledge to provide guidance for the NED/CXO audience in a language, granularity, and style they can understand and apply. Whilst frameworks such as COBIT provide a broad outline of key processes for managing technology risk, they fall short of specifying models, measures, and activities on which this audience should specifically focus (Harmer, 2013). The terminology in many of the ISO/IEC, NIST and CISM frameworks is largely technical, and there is a lack of lexicon that maps this to the language of the NED/CXO audience. This translation is often left to various risk and audit SMEs, without any consistency across the industry and businesses. Recent surveys of this audience ASX/ASIC (2017, p. 20) demonstrate the lack of understanding when only 34% of the companies in the ASX 100 have a cybersecurity risk appetite clearly defined and understood, and "most respondents have either not defined or only partially defined their cyber risk appetite."

[2] Artefact in this instance is assumed to be a standard, framework or accreditation that relates to cybersecurity

This gap in addressing the needs of the NED and CXO stakeholders through standards and frameworks is further compounded by difficulties observed in limited guidance by way of models and metrics that can help this audience.

2.5.3 Models and Metrics

Models in business lexicon that assist NEDs to establish the cybersecurity risk appetite, select the right standards, and then establish the right metrics are limited. Whilst (Cebula et al., 2014) suggest a taxonomy that can be applied to some areas of cybersecurity, it stops short of including people, culture and the behavioural aspects of cybersecurity. Furthermore, the linkage of metrics, key processes, and lexicon has not been covered. An integrated framework for senior business leaders consisting of lifecycle guidance, risk taxonomy, metrics, and culture dimensions is absent in the literature. This gap is also evident from an industry perspective. Gartner research Proctor (2021b, p. 2) states that it "reviews hundreds of metrics programs each year from organizations of every size, in every industry, globally, and the patterns are clear. Almost none of these organizations are effectively measuring and reporting outcomes, and no organization is effectively using outcomes to guide their investment". This challenge is compounded when factoring in regulatory compliance requirements, such as those from APRA (in financial services), which mandate that Senior Executives understand the posture of their cybersecurity, and that Boards are directing and governing this in an appropriate way.

2.5.4 Synthesis and Insights

Cybersecurity governance entails the alignment of the cybersecurity strategy to the business strategy and risk appetite of the organisation. Legal and industry regulation now imposes penalties and criminal proceedings upon entities who have not fulfilled their cybersecurity responsibilities. Unfortunately, much of the collateral, whether that is in the academic or industry frameworks and standards, is aimed at individuals with an existing knowledge of cybersecurity. Furthermore, there is a lack of models that can translate concepts between key stakeholders. These elements highlight the importance of further research and study into this important field in the digital-dependent world in which businesses and governments operate.

2.6 Current Challenges

The variability in the definition of cybersecurity across dictionaries, literature, and industry has created ambiguity in its scope for stakeholders. Similarly, the governance of cybersecurity at the Senior Executive and Board levels is complex due to industry regulations, policies and standards being relatively high level, with linkages to the underlying technical cybersecurity posture being undefined or left to each organisation. At the other end of the spectrum, standards are targeted at a technical audience with limited business lexicon to align to the intent of risk appetite statements. These aspects make cybersecurity governance difficult when discussed in relation to a subject that is relatively new, highly technical, constantly changing through sophisticated attacks, and is faced with new technology of which stakeholders need to stay abreast. This landscape of challenges for NEDs and CXOs is depicted in Figure 12.

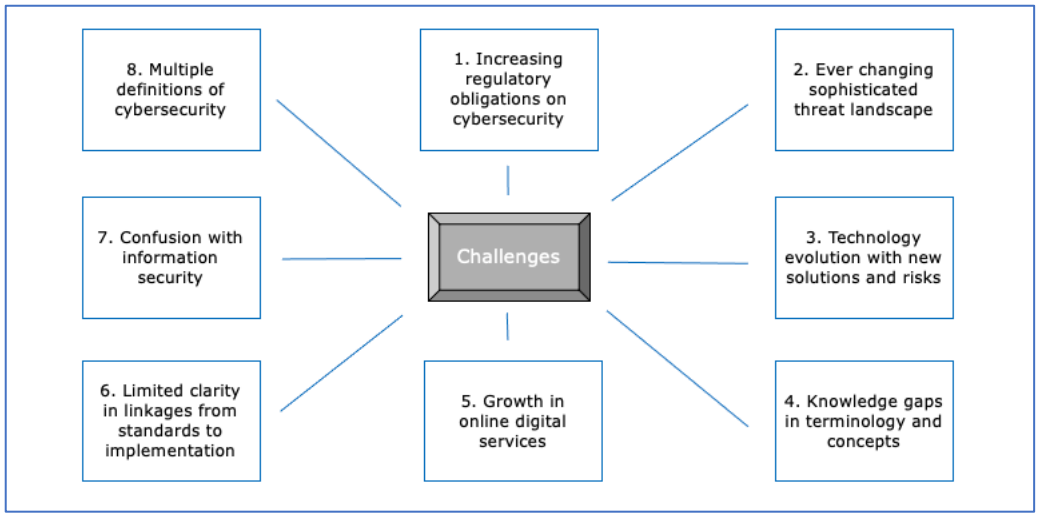

Figure 12: Challenges faced by NEDs/CXOs in the context of cybersecurity governance

These challenges are supported by a range of reference points, with the key ones noted in Table 12.

Challenge #	Challenge Description	Literature references
1	Increasing regulatory obligations	(Haislip et al., 2021; Walton et al., 2021)
2	Sophisticated threat landscape	(Li et al., 2019; Pienta et al., 2020)
3	New technology solutions and risks	(Brown et al., 2017; Walton et al., 2021)
4	Knowledge gaps	(Kappelman et al., 2020; Nolan & McFarlan, 2005)
5	Growth in digital services	(Gielens & Steenkamp, 2019; Guthrie et al., 2021)
6	Limited linkages to implementation	(Iden & Eikebrokk, 2013; Lee et al., 2016)
7	Confusion with information security	(Rout, 2015; von Solms & van Niekerk, 2013)
8	Multiple definitions of cybersecurity	(Cains et al., 2021; Craigen et al., 2014)

Table 12: Reference points for challenges faced by NEDs/CXOs

These identified challenges result in a range of problems when it comes to NEDs and CXOs governing cybersecurity. The variability in the definition of cybersecurity and the confusion in the industry amongst cybersecurity and information security manifests in much debate and discussion. A case in point is auditors initiating audits in both fields, and then having to resolve overlaps with management, which creates delays and complexity. This practice has been widespread in recent years in industry audit plans. Furthermore, reaching agreement on which metrics should be used to track the cybersecurity risk posture also remains largely undefined, with organisations having to identify and agree on these themselves. As a result, risk appetite statements often contain limited dimensions for cybersecurity. This is confirmed in ASX/ASIC (2017) where only 34% of Boards have a clearly defined risk appetite for cybersecurity. One factor in this is the lack of an industry pattern or model to start on, which makes adoption slow and difficult. This situation results in a variability in metrics and indicators across organisations, with a lack of consistency even within one industry sector. The issue is compounded in value chains where some level of governance is required across an eco-system of interconnected organizations, requiring the interface in cybersecurity at the boundaries to be defined and consistent. This value chain is where regulators APRA (2019) are now demanding that third-party risk is managed with more rigour across the supply chain, with metrics and assurance spanning the ecosystem in which each company operates. For companies that are service providers in the value chain (supporting multiple organizations), this results in them having to report and comply to many permutations of metrics and reporting requirements from upstream organizations, even to the same standard such as CPS234 (APRA, 2019). A more standardised cybersecurity governance framework for identifying risk, focus areas and assurance mechanisms would assist in providing a starting point for improved governance at Board levels. This level of framework has not been seen in the literature reviews. It is important however in the formulation of such a framework that the prior literature guides the scope and approach that remains unaddressed to date and that artefacts are developed and evaluated through extensive structured engagements of industry and subject matter experts from academic, government and commercial sectors.

2.7 Research Question

Given the importance of the confidentiality, integrity and availability of data in the digital economy, further assistance to NEDs would help create more trust and confidence in the organizations they govern. As outlined previously in this chapter and covered in more detail in the literature review in Chapter 3, this stakeholder group is not served well by way of practical frameworks and models that give them more confidence in governing the posture of cybersecurity risk. A cybersecurity framework targeted at the NEDs will enable them to better govern cybersecurity with facts and confidence than they are able to presently. If such a framework is adopted across organizations over time, it is likely to introduce a greater standardization of approaches across industry in cybersecurity governance. So, the critical imperative is centred on determining the nature of such a framework through industry engagement and academic rigour.

This study builds on and contributes to the work in cybersecurity governance with additional insights and knowledge being developed for NEDs and CXOs in the form of a Board Cybersecurity Governance Framework (BCGF). This will complement the existing literature that is primarily aimed at the security and risk professional. The BCGF will be informed through research, interviews, relevant theories, an expert evaluation workshop, and a detailed survey of workshop participants.

The core Research Question (RQ) posed for this research is:

> *What framework should be developed to help non-technical audiences such as Board Directors and Senior Executives better govern cybersecurity?*

This RQ is divided into three key sub-questions that are detailed in Section 2.8 with the aims, objectives, and deliverables:

1. What are the key components of this framework that can explicitly address the gaps seen for Board Directors and Senior Executives in a systematic and practical manner?
2. How should each of these components be used in practice by the Board of Directors as they interact with management to set the strategy, risk appetite and tone for cybersecurity?
3. How can the framework allow the Board of Directors to maintain an ongoing knowledge and awareness of the cybersecurity risks and terminology that remains current and relevant?

The focus of the RQ and sub-questions is narrowed down intentionally to a specific audience, namely Board Directors and Senior Executives, which is identified as a gap in the current body of knowledge. This audience is not served as much as the security practitioner in the form of guidance through standards and frameworks; the principle-based literature that is widely available for NEDs and CXOs stops short of this level of guidance. This chapter and the literature review in Chapter 3 supports this assertion.

2.8 Research Aims, Objectives and Deliverables

The sub-questions are detailed in Table 13 along with the accompanying aims, objectives and deliverables for each of these.

Research sub-questions	**Aims**	**Objectives**	**Deliverables**
What are the key components of this framework, that can explicitly address the gaps seen for Board	Identify, formulate, and refine (through interviews and expert workshop and expert survey) the core	The components should be targeted at Board Directors in terms of the activities they	An overarching Board Cybersecurity Governance Framework (**BCGF**) that depicts the core activities, deliverables, and approach for NEDs in governance of cybersecurity risk.

Directors and Senior Executives in a systematic and practical manner?	components of the framework.	undertake, and the language used by them.	The **models** in this should cover the cybersecurity lifecycle and be adaptable for application in various organizations.
How should each of these components be used in practice by the Board of Directors as they interact with management to set the strategy, risk appetite and tone for cybersecurity?	Formulate a set of guidelines on usage of the framework and how this can be made fit-for-purpose for organizations.	The components should be practical in nature and easily adaptable if required for a specific risk profile or industry.	Each model in the BCGF will have **guidelines** on usage. This will include why a model is relevant (its purpose and importance), which pain point it addresses, the inputs/outputs, and how to apply the model in practice.
How can the framework allow Board Directors to maintain an ongoing knowledge and awareness of the cybersecurity risks and terminology that remains current and relevant to them?	Highlight components of the framework that can assist in ongoing awareness and education of focus points that are important for the Board.	Provide means to focus education and awareness onto areas that are relevant and important for the organization.	Specific models that enable an ongoing approach to identify cybersecurity topics, which then informs the education curriculum agenda for NEDs and CXOs.

Table 13: Research sub-questions, aims, objectives and deliverables.

2.9 Summary

This chapter provided the necessary conceptual foundation, research background and problem statement for the research topic in hand. It covered the conceptual foundations, the cybersecurity implementation methods, and the core elements of cybersecurity governance at a Board level. The research question, aims, objectives, and deliverables of this study were also outlined based on the analysis of the related work. The next chapter builds on Chapter 2 and extends the literature review with a view to identifying prior material and the extent to which this informs this study by providing input or a starting point for developing a framework for Board-level cybersecurity governance especially targeting NEDs and CXOs.

3 Literature Review

3.1 Introduction

The previous chapter outlined the research background and problem statement, including the conceptual foundations, the cybersecurity implementation methods currently being used, and the core elements of cybersecurity governance at a Board level. It also provides the research question, aims, objectives, and deliverables of this study. This chapter outlines the literature review conducted to identify the existing studies and the extent to which this can inform the research by providing input or a starting point for the proposed BCGF development, specifically for NEDs and CXOs as per the scope of this research, which is to address the RQ "What framework should be developed to help non-technical audiences such as Board Directors and Senior Executives better govern cybersecurity?"

3.2 Literature Review Method

3.2.1 Approach

A comprehensive literature review was conducted to review and analyse the existing work in the domain of cybersecurity governance as related to NEDs and CXOs. The approach for this review has been informed and shaped by Okoli and Schabram (2010) through an eight-step process that is specifically tailored for information systems research. This approach places importance on rigour and detail in planning research at the outset. This planning encompasses coverage of the purpose and intended goals of the literature review, the selection of literature with clear criteria on what is included and what is excluded, the extraction of literature in terms of the rules to screen the papers, and finally the conclusion of the review covering analysis of the findings with recommendations for the future.

3.2.2 Purpose of review

The aim of the literature review is to specifically identify prior papers targeted at NED and CXO stakeholders in terms of helping them to govern the posture of cybersecurity with more confidence. This included research that depicted the level of comfort they have in fulfilling this responsibility, and the areas that were covered well and those that were not covered for them. This analysis would then inform the nature of the cybersecurity framework that would help them, and elements of this that were critical in order to be of practical application and use in industry.

3.2.3 Sources of literature

This review covered reputable journals and key mainstream business and industry sources that are renowned for papers of a high quality and are impactful to shape applied work in industry. The inclusion of these business and industry sources was warranted, given the momentum in the business literature to document a range of approaches for Boards and Senior Executives, in light of a number of reported breaches that have increased the importance of cybersecurity (APRA, 2019, 2023; ASIC, 2015, 2020). The scope of the literature included the AIS Basket of Eight prestigious IT Journals (S#1-S#8), along with a select number of additional good quality and relevant journals (S#9-S#11), and industry literature (S#12-S#14) to compliment the academic work as noted in Table 14. This was done to ensure that relevant work and insights are not overlooked.

Source Number (S#)	Name	Type
1.	European Journal of Information Systems (EJIS)	Bask of Eight Journal
2.	Information Systems Journal (ISJ)	Bask of Eight Journal

Source Number (S#)	Name	Type
3.	Information Systems Research (ISR)	Bask of Eight Journal
4.	Journal of the Association for Information Systems (JAIS)	Bask of Eight Journal
5.	Journal of Information Technology (JIT)	Bask of Eight Journal
6.	Journal of Management Information Systems (JMIS)	Bask of Eight Journal
7.	Journal of Strategic Information Systems (JSIS)	Bask of Eight Journal
8.	International Journal of Information and Management (IJIM)	Bask of Eight Journal
9.	Journal of Information Systems (JIS)	Other Journal
10.	MIS Quarterly Executive (MISQE)	Other Journal
11.	International Journal of Information and Management (IJIM)	Other Journal
12.	Gartner	Industry Source
13.	Harvard Business Review (HBR)	Industry Source
14.	McKinsey	Industry Source

Table 14: Sources of literature

Industry literature sources (S#12-S#14) were selected due to their strong reputation in business and industry in offering sound practical insights for senior leaders and decision makers. They are regularly referred to in industry and cover the leadership challenges businesses face in a range of topics. Cybersecurity has been an increasing theme in recent years. Gartner offers independent research insights to industry in regard to technology choices and decisions. It prides itself on independency and objectivity that are grounded on peer and quality reviews. HBR and McKinsey articles follow a similar ethos and offer insightful articles to assist current real-life business and industry problems in a practical manner. Collectively these industry sources compliment the research rigour found in papers arising from academic journals (S#1-S#11).

3.2.4 Candidate Papers

The literature review identified relevant papers over a seven-year period from 1 January 2016 to 31 December 2023. This time frame was chosen as it spans a period that has had a greater focus and literature coverage on cybersecurity governance than preceding years, given the changing nature of this field. To classify the candidate papers in a logical manner, *cybersecurity dimensions* as they relate to the Board of Directors are used, as shown in Figure 13. These dimensions have been derived from concepts outlined in Cyber Security Governance Principles issued by the Australian Institute of Company Directors (AICD, 2022a). Details of the mapping are depicted in Appendix 8.1.

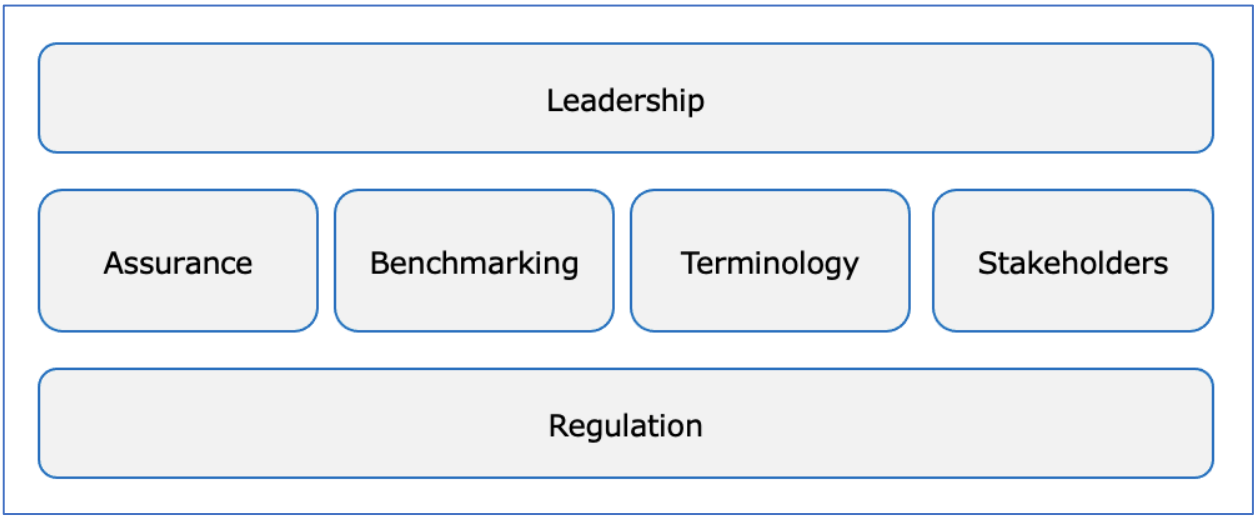

Figure 13: Cybersecurity dimensions

The search terms to identify candidate papers are shown in Table 15.

Cybersecurity Dimension	Primary search domains	Secondary search domains / synonyms	Search Reference (SR) #
Leadership	"cybersecurity" or "cyber security" or "information security"	"governance" or "reporting" or "assurance" or "leadership"	SR#1
Assurance	"cybersecurity" or "cyber security" or "information security"	"health" or "maturity" or "index"	SR#2
Benchmarking	"cybersecurity" or "cyber security" or "information security"	"metrics" or "ratios" or "indicators"	SR#3
Terminology	"cybersecurity" or "cyber security" or "information security"	"lexicon" or "ontology" or "concepts"	SR#4
Stakeholders	"cybersecurity" or "cyber security" or "information security"	"directors" or "Boards" or "executives"	SR#5
Regulation	"cybersecurity" or "cyber security" or "information security"	"standards" or "regulation" or "regulator"	SR#6

Table 15: Search terms applied to identify candidate papers

The rationale for the primary search domains stem from a gradual shift of the terminology from "information security" to "cybersecurity" (Warner, 2012), along with a lack of consistency seen in the use of these terms in the literature, industry and businesses (Craigen et al., 2014). The secondary search domains represent synonyms for the cybersecurity dimension in the prior literature. Only literature that includes a focus on cybersecurity governance for NEDs and CXOs is selected for inclusion, along with literature that focuses on bridging the language divide between this audience and the cybersecurity technical community. Literature that is targeted at a technical audience alone and would not enrich a framework for utilization by Board Directors or business executives is excluded.

3.2.5 Filtering Papers

The identification and filtering of papers followed a series of stages, as shown in Table 16.

Stage	Description	Output
S#1	Identifying journal papers matching the stated search terms without any form of filtering.	Stage 1 papers
S#2	Reviewing Stage 1 papers by examining the title, abstract and skimming the papers for screening purposes. It is necessary to skim the papers to identify even small but relevant insights.	Stage 2 papers
S#3	Comprehensively reading the Stage 2 papers to identify those that provide useful knowledge in the context of the problem statement. This includes removing duplicate papers that appear in multiple search criteria.	Stage 3 papers
S#4	Examining Stage 3 papers and looking at papers listed in the list of references by examining the title and abstract, and skimming. The intention of this stage is to examine upstream references which were not picked up using the original search terms in Stage 1, that may prove to be useful in addressing the problem statement.	Stage 4 papers (also known as upstream papers)

Table 16: Stages in literature review

The overall approach to this four-stage filtering is illustrated in Figure 14. Stage 3 & 4 papers are then analysed to synthesise the key concepts, focus areas, gaps, and insights to build future research and knowledge.

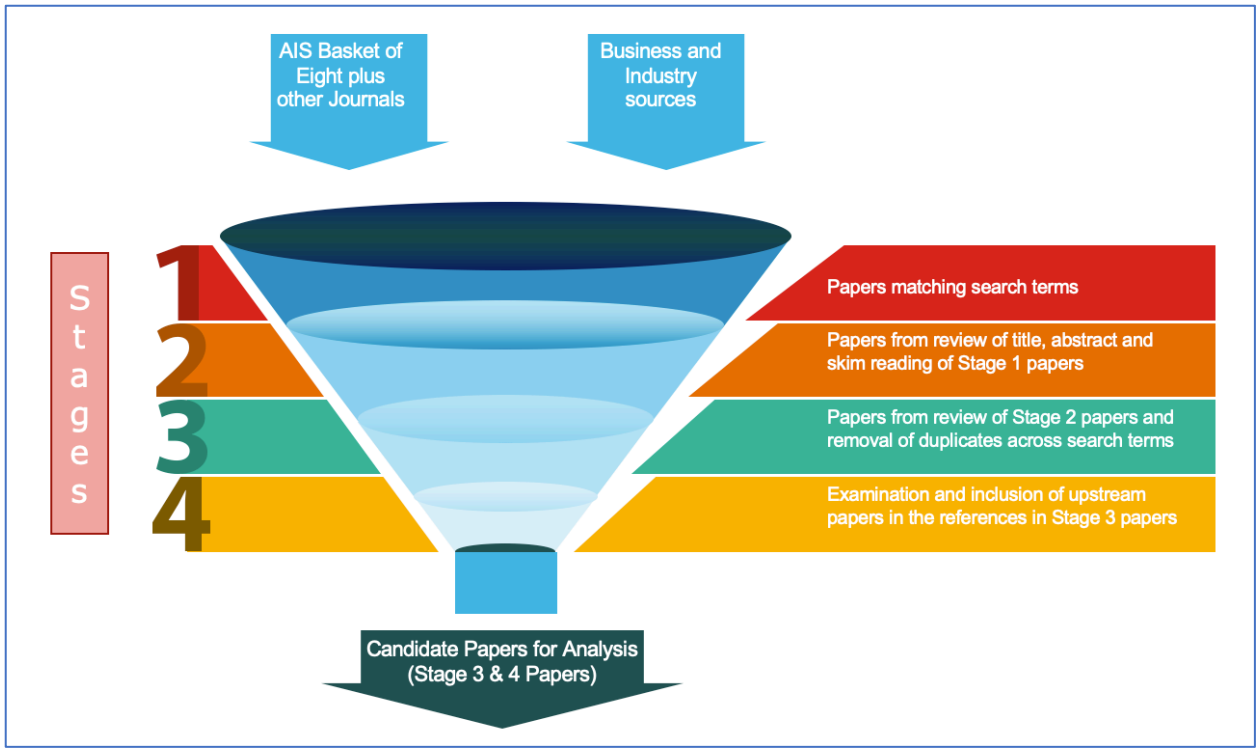

Figure 14: Stages of literature review

3.3 Literature Review Findings

3.3.1 Stage 1-4 Filtering

Stage 1 - The search terms specified in Table 15 in Section 3.2.4 were executed in the selected journal databases to retrieve the initial set of papers for analysis. This stage did not involve any filtering of papers and the results (3,928 papers) for the six search dimensions are shown in Table 17.

Journal	Search Terms					
	SR#1	SR#2	SR#3	SR#4	SR#5	SR#6
EJIS	87	39	47	39	67	81
ISJ	67	47	28	41	33	39
ISR	54	53	23	17	70	30
JAIS	194	153	106	106	179	91
JIT	44	30	17	20	24	34
JMIS	116	80	75	51	92	91
JSIS	45	20	21	20	21	24
MISQ	46	48	25	26	41	27
IJIM	211	126	109	118	72	146
JIS	97	29	39	21	61	78
MISQE	25	2	4	3	47	11
	986	627	494	462	707	652
					Total Papers	3,928

Table 17: Stage 1 search output

As shown in Figure 15, the majority of papers are retrieved from three journals, JAIS, JMIS and IJIM.

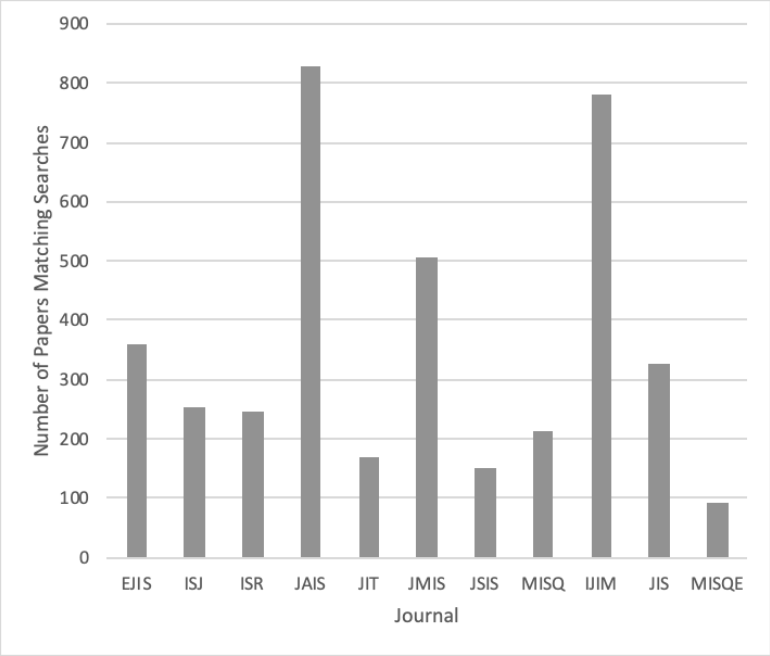

Figure 15: Papers retrieved in stage 1 by journal

Stage 2 - This stage involved a review of the Stage 1 papers by examining the title and abstract and skimming the papers for screening purposes to identify papers relevant to the research statement or those that could be used to build upon if they were related to cybersecurity governance for NEDs or CXOs. Table 18 outlines the results from this filtering which reduced the number of papers from 3,928 to 229.

	SR#1					SR#2				SR#3				SR#4				SR#5				SR#6			
Journal	Governance	Reporting	Assurance	Leadership	TOTAL	Health	Maturity	Index	TOTAL	Metrics	Ratios	Indicators	TOTAL	Lexicon	Ontology	Concepts	TOTAL	Director	Board	Executive	TOTAL	Standards	Regulation	Regulator	TOTAL
EJIS	3	0	0	0	3	0	1	3	4	0	0	1	1	0	1	1	2	0	0	0	0	2	4	2	8
ISJ	0	0	0	1	1	1	0	0	1	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0	1
ISR	1	0	1	1	3	1	1	0	2	0	1	1	2	0	0	1	1	1	1	3	5	1	2	1	4
JAIS	1	1	1	2	5	1	1	0	2	0	0	1	1	0	0	3	3	0	2	2	4	3	1	1	5
JIT	1	1	0	1	3	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	3	0	1	0	1
JMIS	3	14	1	1	19	5	3	7	15	4	0	7	11	0	0	5	5	4	3	6	13	4	3	5	12
JSIS	1	1	1	1	4	1	0	0	1	0	0	0	0	0	0	2	2	0	0	3	3	1	3	0	4
MISQ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	1	0	0	1
IJIM	2	4	0	1	7	1	0	2	3	0	3	3	6	0	1	6	7	1	4	4	9	0	4	0	4
JIS	4	1	1	0	6	0	1	0	1	0	0	1	1	0	0	1	1	2	3	1	6	0	2	0	2
MISQE	4	2	0	2	8	0	0	0	0	0	0	0	0	0	0	0	0	2	2	3	7	0	1	1	2
TOTAL	20	24	5	10	59	10	7	12	29	4	4	14	22	0	2	21	23	11	16	25	52	12	22	10	44
																								Total Papers	229

Table 18: Stage 2 output after filtering

An interesting observation at this stage was the relatively low number of papers retrieved for search #2, #3 and #4 (Assurance, Benchmarking, and Terminology). This set of searches (as shown in Table 18) deals with the health, maturity and measurement of common cybersecurity metrics or ratios with a common lexicon. Figure 16 summarises the results of this stage.

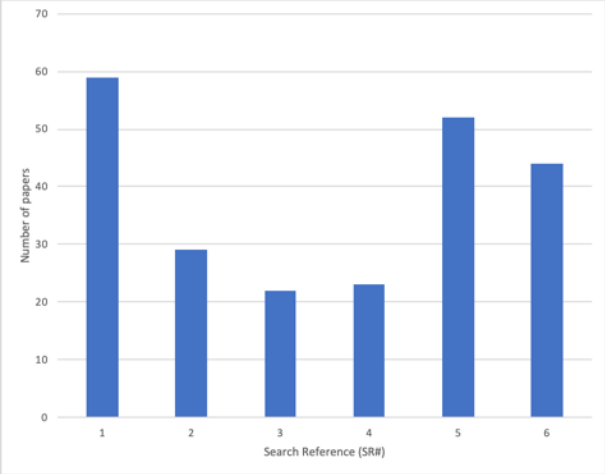

Figure 16: Remaining papers after filtering by search reference

Stage 3 - This stage involved removing the duplicate papers that appeared in multiple search criteria so that they are only counted once in the search term to which they primarily align. Table 19 outlines the results from the de-duplication.

Journal	Search Terms					
	SR#1	SR#2	SR#3	SR#4	SR#5	SR#6
EJIS						
ISJ						
ISR						
JAIS						
JIT						
JMIS	59	29	22	23	52	44
JSIS						
MISQ						
IJIM						
JIS						
MISQE						
	59	29	22	23	52	44
					Total Papers	229
					After removal of duplicates across search terms	52

Table 19: Stage 3 output after removal of duplicates

Following this de-duplication, the remaining 52 papers were carefully reviewed and analysed to ascertain which of these address the research statement directly or indirectly as useful background knowledge to support further research. This initial classification did not eliminate any papers, but highlighted those papers that inform the research statement directly and therefore warranted further detailed analysis.

Stage 4 - In this stage, the references listed in the stage 3 papers were examined by skimming the title and abstract to ascertain whether they should be added to the stage 3 output for further analysis and synthesis. The intention of this stage was to examine the upstream references which were not picked up in the original search terms in Stage 1 and which may prove useful in addressing the problem statement. These upstream papers (12) were added to the papers from stage 3.

3.3.2 Final Candidate Papers

Table 20 represents the final candidate papers identified for analysis, comprising 52 papers from Stage 3 and an additional 12 upstream papers (termed Stage 4 papers) found in the references of the Stage 3 papers. Each paper was analysed using GT techniques to extract the key concepts to aid the analysis and synthesis. For example, concepts such as regulator, cost, breach, reporting and consistency were

extracted from SR#1 as noted in Table 20. This also included categorising each paper on the extent to which it is directly or indirectly relevant to the problem statement, and a synthesis of key insights in a narrative form.

	Reference	Primary Search Term	Key concepts represented	Relevance - D - Direct, or I - Indirect	Insights synthesised in narrative form
1	(Albawaba, 2017)	SR#1	Regulator, Cost, Breach, Reporting, Consistency	D	Costs of breaches, as detailed in an IBM/Ponemon study, are lower in jurisdictions that have a centralised regulatory framework (Europe), whilst where there is uniqueness per state (USA), costs are much higher. This governance model has bearing on organizations with multiple divisions across geographies or product lines. Promotes the need for consistent agreed reporting requirements across separate entities that ultimately roll-up to the same accountability point as a way of managing costs and ensuring consistency in reporting.
2	(AICPA, 2018)	SR#1	Board, Governance, Reporting, Assurance, Controls	D	Contains a high-level reporting framework for Boards/Audit Committees to follow. This covers management, description of the cybersecurity program, management assertions on compliance, and practitioners' opinions on control effectiveness to meet the program's objectives. This is based on the view that there is no widely accepted approach or standard that guides security assessments, and the demands from risk management efforts in this area have led to many disparate cybersecurity frameworks and standards with guidance on how and when to apply them.
3	(AlDaajeh et al., 2022)	SR#1	Governance, Reporting, Education, Goals, Strategy	D	Analyses a number of national cybersecurity plans across various countries and proposes an approach to formulate what it calls a 'goal-question-outcomes+strategy' approach to formulating education and training programs at a national level. This analyses the goals of each strategy and identifies 'clusters' of education areas. This has bearing on NEDs as a similar pattern could be relevant for them to frame the curriculum across current and emerging risks. This would enable a just-in-time approach to learning that aligns to business strategy goals and risks.
4	(Anderson et al., 2017)	SR#1	Reporting, Assurance, Assets, Ecosystem	D	Discusses getting the right security controls on information that may be shared amongst other parties. Covers the need to balance this in a connected world. Has relevance to Board Directors, as they identify the 'crown jewels' they need to protect and when these become openly available (legally) in the value chain to other parties in the ecosystem, and therefore require less security.
5	(Banker & Feng, 2019)	SR#5	Executive, Reporting, Assurance, Breaches	D	Makes use of Ponemon framework to classify security breaches into 3 causes, namely (1) system deficiency, (2) criminal fraud, and (3) human error. Argues the case that CIO turnover is greater when there is a system deficiency that causes a breach, whereas for fraud and human error, the turnover of the CFO or other CXO is much lower. This has a bearing on reporting the security posture of the technical aspects, so that NEDs and business CXOs are more informed on the coverage and effectiveness of technical security controls. Could inform the manner in

	Reference	Primary Search Term	Key concepts represented	Relevance - D - Direct, or I - Indirect	Insights synthesised in narrative form
					which assurance and metrics are described for executives and Board Directors.
6	(Baxter et al., 2016)	SR#1	Governance, Compliance, Gamification, Scoreboard, Culture	D	Suggests use of gamification practices (e.g. leaderboard, recognition) to improve security awareness, participation, and engagement. This could inform cybersecurity culture imperatives that rely on metrics on improving awareness and education. Would help to address the risk of people often being the weakest link in cybersecurity.
7	(Brown et al., 2017)	SR#1	Governance, Culture	I	Posits that the professional values, integrity, and virtues (including culture) are important to ensure good security ecosystem. This has some relevance in approach to setting the right tone in cybersecurity culture and having ways to measure the state of the culture. However, there is limited guidance on how NEDs or CXOs can implement the insights in the paper that highlight the importance of integrity and ethics.
8	(CAQ, 2018)	SR#1	Governance, Metrics, Assurance, Board, Questions	D	Principle-level guidance from the Centre of Audit Quality which includes a series of questions for NEDs to ask when managing cybersecurity risk. This is limited to risks underpinning financial audits, and not on broader operational risk. The categories of questions focus on the auditor, management disclosures, and management's approach to cybersecurity management. Whilst a useful aid that promotes the need to ask questions, the scope is limited in breadth and also provides limited guidance on the how NEDs can embed these to set the tone on what they deem as expectations from cybersecurity in their firm.
9	(Cheong et al., 2021)	SR#6	Regulator, Breaches, Reporting	D	Framework for reporting to regulators such as the Securities and Exchange Commission (SEC), including root causes of issues. Offers some insights on disclosure reporting from management to Boards, and then to external actors.
10	(Cram & D'Arcy, 2023)	SR#6	Standards, Regulation, Compliance, Culture	I	Contends that compliance to cybersecurity policies relies on encouragement (rewards) and employee characteristics (attitude) to drive the right behaviour and culture. This introduces the concept of cybersecurity legitimacy as an area that includes convincing employees that the initiatives are fair and reasonable. It argues that if you want to drive up compliance, this is as important to encourage the right behaviour/culture.
11	(Cram et al., 2021)	SR#1	Governance, Leadership, Metrics	D	Outlines signs of security fatigue in an organization where stakeholders may not see the red flags. Covers how to detect and aim to minimise this. Has relevance to the proposed framework to ensure metrics are meaningful, provide insight, and not just a wow factor (e.g. # of attacks a minute on website).
12	(Cram et al., 2017)	SR#6	Index, Assurance, Standards, Policy, Compliance, Culture	D	Covers research into information security policies and argues the case that a generic framework of these is not available, and through this, proposes common areas and relationships that should be covered. These areas include the core design of policies, the influence of these on employees, the compliance aspects, and finally the linkage to organization objectives. Whilst the paper does not

	Reference	Primary Search Term	Key concepts represented	Relevance - D - Direct, or I - Indirect	Insights synthesised in narrative form
					focus on NEDs per se, the approach to correlating policy through relationships (and drawing upon relevant theories to back this up) offers a pattern to depict the line of sight from a Board-level framework to the lower-level management implementation of this, through the use of relationships.
13	(D'Arcy & Basoglu, 2022)	SR#6	Standards, Regulator, Breach, Incident, Disclosure,	I	Presents research that supports the case that disclosures to the regulator are timelier and contain relevant information if these are external in nature and influenced by public pressure. Internal incidents and risks tend not to have same urgency or focus, until they become public. This has a direct correlation on the risk appetite for NEDs in terms of setting the thresholds and parameters on the nature of incidents and then the handling of these. This manifests in the 'response' stage of the security lifecycle but needs agreement well before when standards and risk appetite are agreed.
14	(Dhillon et al., 2021)	SR#6	Regulation, Compliance, Standards, Incident, Implementation	I	Analyses prior information systems security literature and explains where the focus of the community has been and what gaps remain. Identifies that academic literature is centred on behaviour, privacy, and compliance, whilst the practitioner places importance on security attacks. Proposes that a future research agenda should focus on security attacks, system design and vulnerabilities and compliance/behaviour. The research is limited in its form and is only targeted at the implementation stakeholders. Stakeholders, such as NEDs and CXOs, that govern cybersecurity in the Boardroom are not covered in this research.
15	(Doynikova et al., 2019)	SR#4	Ontology, Metrics, Concepts	I	Analyses a series of security management ontologies and proposes from these a high-level ontology map of potential concepts/classes that could form metrics if taken to a more detailed level. The authors state this is the start of their research and further extension is planned to an implementation level. They do not provide guidance on how such an ontology map could be stay relevant and fit-for-purpose given many metrics evolve over time as the maturity of an organisation changes, and as technology evolves to provide greater variety and velocity in data points.
16	(Dupont et al., 2023)	SR#1	Governance, Incident, Response	D	Talks to cyber-resilience as a way to withstand shocks arising from breaches and suggests twelve categories or measures of cyber-resilience. These offer some relevance to NEDs as they are organised into strategic and operational, and those that are strategic (compliance, situational awareness, governance, market position and finance) could inform a model for risk appetite statements for Boards. This would be an extension of the authors' research.
17	(Evans & Price, 2020)	SR#5	Board, Executive, Assets	I	Covers the use of a Holistic Information Asset Management (HIAM) model to better govern digital assets. Some concepts could be extended to cover cybersecurity dimensions of assets that require protection.

	Reference	Primary Search Term	Key concepts represented	Relevance - D - Direct, or I - Indirect	Insights synthesised in narrative form
18	(Gale et al., 2022)	SR#1	Governance, Board, Engagement, Skills	D	Argues from research that NEDs are not as engaged in cybersecurity as other areas of oversight. Authors argue that regulation is the factor that is most influential in driving this engagement, and that the background and skills of a director determine their engagement level in cybersecurity, with an over-reliance on a single Board member to take this up. Offers a series of recommendations that include regulation and reporting to drive up skills and engagement of NEDs.
19	(Haislip et al., 2021)	SR#2	Governance, Health, Indicator, Executive	I	Discusses that breaches cannot be mitigated by one CXO alone but is a shared responsibility for top level management such as the CEO, CFO and CIO. Argues the case that when such stakeholders have more IT expertise then the number of breaches is reduced. The insights are limited to CXOs and do not offer any guidance on NED engagement or how this stakeholder is impacted by better CXO capability in terms of how they engage in the language that is more appropriate for the Boardroom.
20	(Higgs et al., 2016)	SR#5	Board, Executive	I	Suggests use of a Board Technology Committee to manage cybersecurity posture and breaches, and how this has assisted companies to minimise breaches. Skills and focus on this topic in such committees has linkages and some evidence in enabling meaningful fit for purpose frameworks.
21	(Jensen et al., 2022)	SR#4	Gamification, Reporting, Concepts, Culture	D	Authors conducted research and experiments to identify the extent to which gamification of phishing results could improve the reporting of such attempts and also reduce the risk to the organization. Provides some useful insights on a leaderboard approach to gamification that recognises or rewards participant behaviour when it is positive. Enables cultural change and a constructive way for NEDs to request such metrics and reporting across divisions/departments of a company.
22	(Jiawen et al., 2023)	SR#1	Governance, Leadership, Culture, Compliance, Gamification	I	Analyses different leadership styles and draws conclusion that a mix of skills is necessary to improve the understanding of employees of information security compliance and relevant controls. These styles are grounded on leaders actively demonstrating an understanding and importance to cybersecurity matters as a way to promote the right culture, in other words, creating the right shadow.
23	(Kam et al., 2022)	SR#5	Standards, Regulator, Skills, Education	I	Suggests research to increase interest in cybersecurity education and skills development to address the skills gap and shortage seen across the industry and businesses. Whilst the paper does not cover NEDs in terms of their knowledge and education, there are some parallels that could be applied to Boardrooms. This includes providing some perceived learning autonomy through embedding education in existing activities, and also motivational elements that are self-determined by NEDs, such as attaining accreditation points with relevant director institutes.

	Reference	Primary Search Term	Key concepts represented	Relevance - D - Direct, or I - Indirect	Insights synthesised in narrative form
24	(Lee et al., 2016)	SR#6	Standards, Assurance, Executive, Regulation	D	Covers the insight that a single standard does not always have the complete scope for security maturity, and that several will be needed in parallel to address risk. Very relevant discussion for a Board framework.
25	(Leech & Hanlon, 2017)	SR#5	Board, Oversight	D	Board risk chapter provides overview of the difficulties Boards face when managing cybersecurity risk. These include lack of management ownership, failure to link cybersecurity measures to business goals, cybersecurity missing from strategic plans, too much focus on internal controls, and a lack of information on residual risk. Paper offers actions CEOs / Boards can take in this context.
26	(Liu et al., 2020)	SR#1	Regulation, Executive, Board, Governance, Structure	D	Discusses centralised v decentralised governance of IT, and that centralised governance gives better outcomes for reducing risk. Such concepts may offer guidance to NEDs when governing at Board level.
27	(McLaughlin & Gogan, 2018)	SR#1	Governance, Executive, Leadership, Lifecycle, Metrics	D	Useful framework (and references) to structure focus on governance/metrics, in 'before incident' and then 'during or shortly after an incident'. Phases - Prepare, Prevent, Detect, Respond, Learn. Could be useful as a starting point for a Board-level framework that is lifecycle based.
28	(Mehrizi et al., 2022)	SR#6	Standards, Incident, Education	D	Reviews literature to frame how organizations learn from cybersecurity incidents. This includes learning from past experience to draw lessons for the future, learning from present incidents, and also some from future scenario-based incidents. Proposes a high-level framework on learning modes and how these could be applied. This has bearing on NED education as all three approaches could assist, with an additional overlay of external incidents that could be brought into role playing in desktop situations.
29	(Menard et al., 2017)	SR#2	Executive, Reporting, Indicators	D	Provides analysis of Protection Motivation Theory and Self-Determination Theory as it relates to users and their level of compliance. This has some correlation to NED / CXO behaviour in terms of what drives their focus on cybersecurity posture. The approach focuses on the threats to individuals and also the value brought from sound cybersecurity posture.
30	(Mishra et al., 2022)	SR#1	Governance, Policy, Assurance, Benchmark	D	Contrasts national level cybersecurity regulations and policies (in terms of their scope) across a range of countries in an attempt to identify strengths and gaps across these. Identifies a number of attributes (e.g. infrastructure, knowledge and awareness, frameworks, and models, etc) against which the countries are benchmarked. Such a classification is particularly relevant for CXOs when reporting to Boards, as it could offer a way to compare these attributes for peer organizations where data can be attained.
31	(Niemimaa & Niemimaa, 2017)	SR#4	Ontology, Standards, Regulation	D	Useful concepts to translate/transform security standards/policy to an organisational context. Relevant for Boards that may need to insist 'localisation' is done for relevant security standards and policies.

	Reference	Primary Search Term	Key concepts represented	Relevance - D - Direct, or I - Indirect	Insights synthesised in narrative form
32	(Pearlson et al., 2022)	SR#1	Reporting, Metrics, Culture, Recognition	D	A case study to improve cybersecurity culture at Verizon by focusing first on reducing the credential through phishing simulations, increasing reporting from employees on suspect emails, and increasing corporate password manager. Demonstrates that instilling the right culture involves more than training and awareness campaigns. Key is the use of metrics to motivate employees and demonstrate success along the way. Managers were given a dashboard to track their team's progress. Useful for cybersecurity culture change for NEDs to adopt when setting the tone as the paper distinguishes between actions, habits and desired behaviour.
33	(Peppard et al., 2023)	SR#1	Governance, Board, Oversight	D	Overview of the Board role in the oversight of technology / digital investments, including cybersecurity risk. The authors detail issues related to technology-governance amongst NEDS and gaps in capability in NEDS for technology-related decision making. By way of example, only a quarter of FTSE 250 company Boards in the UK have a director with expertise in IT. They go on to detail how Boards can be more effective in a technology-governance role through literacy, Board frameworks, and the right language. They articulate a lack of literature targeted at the Board due to a fact that researchers do not have access to Board data or know-how, and do not have a deep understanding of the topics/issues NEDs grapple with around technology risk. A good framing editorial paper that reinforces the problem statement and introduces some concepts to encourage further research.
34	(Proudfoot et al., 2023)	SR#1	Governance, Board, Executive, Communication	D	Recognises the complexity of oversight and governance for NEDs and identifies four challenges Boards encounter, with 10 recommended actions they can take in response. Four challenges include complacency in recognising the importance of cybersecurity, the NED-CXO interactions being dependent on effective communication from the CISO, lack of Board cybersecurity expertise, and expanding cybersecurity regulations. This recent paper recognised the NED-CXO gap and is one of a few that proposes practical steps these stakeholders can take to improve the effectiveness of cybersecurity governance in the Boardroom.
35	(Safi et al., 2021)	SR#1	Governance, Reporting, Regulation	D	Looks at factors applied to make security investment decisions. Useful questions for Boards to ensure ROI on security investment, and ensuring blind spots are not evident across the lifecycle.
36	(Schuetz et al., 2020)	SR#5	Executive, Reporting, Health, Concepts	D	Discusses how Protection Motivation Theory guides personal and organizational behaviour in security responses. Could be relevant in context of Board Directors making decisions, given they are legally liable for cybersecurity.
37	(Shariffuddin & Mohamed, 2020)	SR#1	Governance	D	Short paper on summarising various security governance frameworks and standards that may be useful for formulating a Board framework.

	Reference	Primary Search Term	Key concepts represented	Relevance - D - Direct, or I - Indirect	Insights synthesised in narrative form
38	(Silic & Lowry, 2020)	SR#1	Assurance, Compliance	D	Uses gamification to increase effectiveness and compliance of Security Education Training and Awareness (SETA) activities.
39	(Slapničar et al., 2023)	SR#1	Governance, Risk Management, Accountability	D	Suggests the extension of the three lines of defence model to five lines of accountability (5 LoA) which includes the accountability of executives and Board of Directors. It then outlines the adoption approaches of the 5 LoA which follow two dimensions – type of interaction (blended/segregated), and then level of engagement (high/low). The authors find that in all permutations of these dimensions, there is room for improvement in terms of minimising cybersecurity risk and no one model offers any advantage. However, accountability become clearer in the 5 LoA, and the paper offers practical paths and steps to help improve cybersecurity governance and accountability based on this research.
40	(Slapničar et al., 2022)	SR#1	Governance, Index, Maturity	D	Identifies a way to track the effectiveness of cybersecurity audits as a means to improve cyber risk management and reduce successful cyber-attacks. Identifies use of a Cybersecurity Audit Index to measure this. Concludes that the index is positively associated with maturity, but it is not related to the probability (or reduction of) a cyber-attack.
41	(Smith et al., 2019)	SR#1	Governance, Audit, Board, Fees	I	Argues the case that breaches impact audit fees and there is variation in this in terms of whether the breach is internally or externally disclosed. Useful to draw the investment case in cybersecurity given the framing of costs in a control environment.
42	(Soomro et al., 2016)	SR#5	Governance, Concepts, Board, Policy	I	Comprehensive literature review of management roles and practices in cybersecurity, and from this, suggests ways to improve the maturity of cybersecurity efforts. Suggests a holistic approach to information security management that includes top-level management, policy development and execution, awareness and training, and involvement of strategic decision makers.
43	(Steinbart et al., 2016)	SR#3	Metrics, Maturity	I	Argues the case that there is no clear way to measure the progress and effectiveness of a security program. Proposes the use of the COBIT framework as one way to identify measures and metrics that can be used to track the effectiveness of cybersecurity programs which is informed by maturity in various IT domains in COBIT. Whilst the authors indicated this approach measures the progress of a cybersecurity program, this is limited in a number of risk management practices and is not comprehensive enough to cover the cybersecurity lifecycle and its nuances that are unique and distinct from general IT controls in COBIT.
44	(Taherdoost, 2022)	SR#1	Reporting	I	Compares and contrasts definitions of cybersecurity and information security, including confusion on the scope and meaning of these. Proposes that cybersecurity is a subset of information security. This contradicts a number of other views (discussed in Section 2.2, Conceptual

	Reference	Primary Search Term	Key concepts represented	Relevance - D - Direct, or I - Indirect	Insights synthesised in narrative form
					Foundation), which state cybersecurity as being a broader domain and information security sitting within this.
45	(Vedadi & Warkentin, 2020)	SR#1	Governance, Leadership, Indicators	I	Talks to herd mentality that is seen in security decisions on occasions when choosing direction and how this changes afterwards. This adds some caution to a Board-level framework which needs to ensure such risks are dealt with explicitly.
46	(Walton et al., 2021)	SR#6	Regulation, Governance, Leadership	D	Contains a holistic systematic literature review of 68 cybersecurity papers, classified across a framework of four cybersecurity dimensions - 1) Disclosure, 2) Investment, 3) Governance, and 4) Market response to incidents. No specific guidance is given in the paper, but it offers a useful synthesis across the dimensions that matter to NEDS and CXOs and provides practical guidance in a consolidated manner (something that is rare in the cybersecurity literature).
47	(Wang et al., 2023)	SR#1	Reporting, Innovation	D	Analyses the linkage between new innovative technology solutions and cybersecurity risk arising from them. Demonstrates increased cybersecurity risk when IT innovations are deployed, even when they may solve or improve another need. Outlines the need to manage such risks explicitly. Relevant to NEDs when governing new technology implementations by ensuring the right risk management skills and processes are in place, and that external knowledge is applied to manage risks.
48	(Wolff, 2016)	SR#3	Concepts, Indicators, Reporting, Board	D	Considers the negative impact in over controlling and specifying controls. For example, overly complex password syntax can result in people writing passwords down. Useful from a Board framework perspective to ensure management direction is pragmatic and does not have unintended consequences.
49	(Yang et al., 2017)	SR#1	Reporting, Operational Risk	I	Uses Action Research to formulate an operational risk framework (for the risk practitioner), including a focus on cybersecurity risk. This examines the impact to the confidentiality, integrity, and availability of information from various events. Useful findings to inform extension of this research for NED / CXO audience in the area of cybersecurity resilience.
50	(Yeoh et al., 2022)	SR#1	Governance, Investment, Critical Success Factors	D	Formulates a critical success factor (CSF) framework that aims to improve the success rate of cybersecurity programs. Proposes 11 CSFs with 79 underlying elements. The CSFs relate to the implementation of cybersecurity by the practitioner and is not aimed at governance stakeholders such as NEDs/CXOs.
51	(Zhao et al., 2019)	SR#3	Metrics, Indicators, Health, Index, Measurement	D	Outlines measurement points across a series of indicators as a means to establish oversight across the Protect, Detect, Respond, and Manage (PDR-M) lifecycle. Whilst this is generic and technical, and also point in time (due to changing nature of technology and measurement points), it does offer a starting point upon which to build upon for NEDs. It would need to be less technical and more generic across organizations to be valuable for Boardroom governance and oversight.

	Reference	Primary Search Term	Key concepts represented	Relevance - D - Direct, or I - Indirect	Insights synthesised in narrative form
52	(Zhuang et al., 2020)	SR#2	Reporting, Index	D	Introduces the concept of a security index that can be used to as an indicator of an organization's security posture. Useful research to build on for a Board-level series of indices.
UPSTREAM References (Stage 4)					
53	(Bailey et al., 2014)	SR#1	Governance, Executives, Reporting	D	Posits that cybersecurity is the responsibility of the CEO and other members of the senior management team, not just the CISO/CIO. Risks span functions, business units, companies, and customers. Leaders should focus on 4 areas in governance spanning strategy, cross-business unit focus, user behaviour, and effective governance and reporting.
54	(CII, 2016)	SR#5	Governance, Board, Reporting	D	Council of Institutional Investors (CII) outlines that cybersecurity is an integral part of a Board's accountability, and they need not develop detailed technical knowledge. They should focus on 5 questions to understand the strategy where weaknesses exist and support informed investment.
55	(Clinton et al., 2020)	SR#1	Governance, Board, Reporting	D	National Association of Corporate Directors details five key principles for Boards to use when they govern cybersecurity, along with some high-level toolkits and examples to bring these to life.
56	(Donalds & Osei-Bryson, 2020)	SR#1	Governance, Reporting, Maturity, Leadership	I	Analyses how leadership styles impact security compliance. Argues that some styles may cause a blind spot and a reluctance to comply with things like password syntax and this can impact culture.
57	(Kayworth & Whitten, 2010)	SR#1	Governance, Strategy,	I	Provides an approach for an effective information security program. Outlines the importance of alignment to business strategy and integration to the social and organizational aspects, in addition to the technical dimensions. Aligns to the view that cybersecurity includes the people and process side of the definition, as much as the technology dimensions.
58	(Kormos et al., 1999)	SR#3	Metrics, Reporting, Governance	I	Presents a brief overview of metrics and how to derive these for different perspectives. Also includes tree diagrams to classify security metrics
59	(Lennon, 2003)	SR#3	Metrics, Reporting	D	Outlines a high-level approach to formulating a security metrics program to track the performance of security and direct decision making.
60	(Nolan & McFarlan, 2005)	SR#1	Governance, Board	D	Posits that Board governance can go a long way toward helping a company avoid unnecessary risk and improve its competitive position. A fit-for-purpose IT governance committee at Board level is necessary.
61	(Payne, 2006)	SR#3	Metrics, Reporting	D	Outlines a simple basic aspects of security metrics, in terms of the characteristics of these and ensuring these are SMART (i.e. specific, measurable, attainable, repeatable, and time-dependent).
62	(Rantos et al., 2012)	SR#3	Metrics, Ratios, Culture	I	Provides a way of measuring the effectiveness of security awareness initiatives over and above a focus on purely completion rates/quizzes. This is a key area for inclusion in the model when it comes to security culture.
63	(Savola, 2007)	SR#4	Lexicon	I	Outlines a taxonomy model for security metrics based on multiple trees.

	Reference	Primary Search Term	Key concepts represented	Relevance - D - Direct, or I - Indirect	Insights synthesised in narrative form
64	(Savola, 2008)	SR#4	Lexicon	I	Outlines a taxonomy model for security metrics based on multiple trees and an approach to defining metrics.

Table 20: Candidate papers from key academic databases

Of these 64 candidate papers, 22 have indirect relevance to the problem/research statement, whilst the remaining 42 are directly relevant and offer some core insights that are synthesised in Section 3.4. The 54 concepts synthesised from the 64 candidate papers using GT techniques are depicted in Table 21 where the top five concepts, (in terms of occurrences and percentage of all concepts), include Governance, Reporting, Board, Executive, and Metrics.

Concept in Literature from Academic Databases	#Occurrences in Academic Literature	% of all Academic Literature Concepts
Governance	31	14.62
Reporting	23	10.85
Board	15	7.08
Executive	11	5.19
Metrics	11	5.19
Assurance	8	3.77
Culture	8	3.77
Standards	8	3.77
Regulation	7	3.30
Compliance	6	2.83
Leadership	6	2.83
Concepts	5	2.36
Indicators	5	2.36
Breach	4	1.89
Incident	4	1.89
Index	4	1.89
Education	3	1.42
Gamification	3	1.42
Health	3	1.42
Maturity	3	1.42
Policy	3	1.42
Regulator	3	1.42
Assets	2	0.94
Lexicon	2	0.94
Ontology	2	0.94
Oversight	2	0.94
Skills	2	0.94
Strategy	2	0.94
Accountability	1	0.47
Audit	1	0.47
Benchmark	1	0.47
Communication	1	0.47

Concept in Literature from Academic Databases	#Occurrences in Academic Literature	% of all Academic Literature Concepts
Consistency	1	0.47
Controls	1	0.47
Cost	1	0.47
Critical Success Factors	1	0.47
Disclosure	1	0.47
Ecosystem	1	0.47
Engagement	1	0.47
Fees	1	0.47
Goals	1	0.47
Implementation	1	0.47
Innovation	1	0.47
Investment	1	0.47
Lifecycle	1	0.47
Measurement	1	0.47
Operational Risk	1	0.47
Questions	1	0.47
Ratios	1	0.47
Recognition	1	0.47
Response	1	0.47
Risk Management	1	0.47
Scoreboard	1	0.47
Structure	1	0.47

Table 21: Occurrences of concepts in academic literature

3.3.3 Industry Sources

Three industry / business sources, namely Gartner, Harvard Business Review (HBR) and McKinsey Quarterly were examined using the same search terms as for the academic literature. Whilst the initial number of papers in these sources appeared to have large coverage in the first pass, upon review and filtering, it was evident that the vast majority were raising the importance to Boards of managing cybersecurity with more focus. Very few articles or papers offered guidance on 'how' this was to be achieved. Further, the distribution of papers into each search term were less relevant given the affinity of most final papers being SR#1 (governance, reporting, assurance, and leadership) and SR#5 (directors, Boards, executives). Table 22 shows the number of papers identified and filtered. All of these were directly relevant to the research problem. As for the papers from academic sources, GT techniques were used to identify key concepts present in the papers.

	Source	# papers initially found	# papers following filtering and review
1	Gartner	773	13
2	HBR	106	5
3.	McKinsey	122	4
	Total	**1,001**	**22**

Table 22: Paper count by industry source

Table 23 depicts the relevant industry papers identified and analysed to inform the literature review with industry insights. As for the papers in academic sources, each paper from industry sources was analysed using GT techniques to extract key concepts to aid the analysis and synthesis.

	Source	Reference	Key concepts represented	Relevance - D – Direct, or I – Indirect	Insights synthesised from narrative
1	Gartner	(Buchanan et al., 2022)	Metrics, Board, Executives, Investment, Decisions	D	It is important to involve business executives in understanding and making decisions on cybersecurity budget. This will enable decisions on coverage and understanding the targets that can or cannot be achieved within the budget. Outcome-driven metrics then enable the forecasting and tracking of the level of protection in place.
2	Gartner	(Iyengar, 2021)	Risk, Risk Appetite, Cyberattack	D	In 2021, 88% percent of respondents from a Board survey say cybersecurity is a broader business risk, rather than just a technology risk. They also see the need to accelerate digital business and increase their risk appetite.
3	Gartner	(Mandy et al., 2021)	Metrics, Decisions, Business, Board	D	Covers the fact that security and risk leaders tend to focus on operational metrics for cybersecurity that have limited value to business stakeholders. Outlines the CARE framework for defining metrics that are meaningful (consistent, adequate, reasonable, and effective). Posits that using this approach to develop a catalogue of metrics will help create more effective stakeholder messaging and give more defensibility to an organization's cybersecurity posture.
4	Gartner	(Olyaei & Mandy, 2022)	Board, Executives, Business Decisions, Outcome Metrics, Reporting	D	States the need for business executives to better understand cybersecurity risk and also be incentivised for this from the Board. Performance-related reports on cybersecurity must then be presented to and be reviewed by the Board. Places importance on third-party risk and internal culture. Positions the CISO role as one that needs to provide leadership on educating CXOs and facilitating risk discussions, so that cybersecurity risk is a business imperative.
5	Gartner	(Olyaei et al., 2021)	Board, Executives	D	Cybersecurity risk is identified as a top source of risk for Board members. Nearly half of CISOs interviewed have a sharp fall in expectations and performance when it comes to engaging executives and Board members. Also covers approaches to engage directors through cybersecurity sub-committees and also ensuring tailored fit-for-purpose approach to assurance in context of the skills and knowledge of the Board.
6	Gartner	(Olyaei & Wheatman, 2020)	Board, Questions, Confidence	D	Boards are realising the criticality of cybersecurity and asking more complex questions. Confidence in an organization's ability to prevent and respond to incidents is low, with only a minority of Board Directors expressing confidence. Covers five typical questions, and the types of responses that should be considered.

	Source	Reference	Key concepts represented	Relevance - D – Direct, or I – Indirect	Insights synthesised from narrative
7	Gartner	(Olyaei & Wheatman, 2022)	Board, Questions, Reporting	D	States that cybersecurity risk management is now increasing at the Board level, with frequent reporting by security and risk executives (90% of those surveyed). However, Board confidence in the cybersecurity posture remains low, with very few Boards expressing confidence in their organisation's ability to prevent and respond to incidents. Recommends CXOs should focus on 5 Board questions that cover the economics of cybersecurity, compliance, adequate reporting, speed of change, and competitive advantage. These prepare CXOs better and helps Boards. Also discusses a balanced scorecard approach to reporting cybersecurity contribution to business performance. Whilst the paper is centred close to the research statement, it primarily focusses on how CXOs can better respond to NED questions, not a framework from the perspective of NEDs. Nevertheless, some areas of this can be inferred to inform targeted artefacts for NEDs.
8	Gartner	(Proctor, 2021a) – Cybersecurity Must Be Treated as a Business Decision	Outcome metrics, Questions, Pitfalls	D	Explains how Boards and executive leaders are asking the wrong questions about cybersecurity leading to poor investment decisions. Also discusses that outcome-driven metrics should be used to create more effective governance over cybersecurity priorities and investments.
9	Gartner	(Proctor, 2021b) – An Outcome-Driven Approach to Cybersecurity Improves Executive Decision Making	Outcome metrics, Board, Executive, Assurance	D	States that executives and Board of Directors struggle to know much cybersecurity is enough and that most organizations struggle to demonstrate the right balance between protecting the business and running the business. Discusses the need to have outcome-driven metrics to measure cybersecurity capabilities.
10	Gartner	(Proctor, 2021c) – Outcome-Driven Metrics for Cybersecurity in the Digital Era	Metrics, Protection, Assurance, Performance	D	Outlines that in the Gartner database in 2020, cybersecurity metrics are mostly trailing indicators of operational results, and not useful to measure the level of protection in place. States that most standards and frameworks for cybersecurity define how to build capability, and not measure its ongoing performance. Defines an approach to outcome-driven metrics for cybersecurity. Interestingly, whilst it provides an approach, it stops short of recommending a catalogue or set of metrics for executives and Board Directors. However, this is probably the closest any paper has been in framing the issue and an approach to solve this generically for some dimensions of the cybersecurity

	Source	Reference	Key concepts represented	Relevance - D – Direct, or I – Indirect	Insights synthesised from narrative
					definition (largely on the technical aspects, with less on culture, behaviour, etc).
11	Gartner	(Proctor & Shankel, 2023)	Metrics	D	Outlines four key steps to develop outcome-based cybersecurity metrics that enable decision making and are more useful in business decisions. These enable actions to be taken and enable discussion on the extent of risk and investment that should be accepted or applied.
12	Gartner	(Scholtz, 2021)	Cost, Benefit, Business Value, Business Drivers	D	Provides guidance on how CXOs can present cybersecurity to Boards better. Cybersecurity presentations do not resonate with senior leaders and the Board and are rarely connected to revenue increase or cost reduction imperatives. Cybersecurity investment is seen as a necessary evil rather than a business investment. Provides an approach that explains linkage between business drivers and cybersecurity impacts (positive and negative).
13	Gartner	(Witty & Hoeck, 2022)	Board, Resilience, Incident, Response, Continuity, Breach	D	Details the large impacts on operational resilience from cybersecurity attacks in recent years. This can cease the services of an organization for many days and weeks. Discusses the need for Boards and executives to ensure the business continuity and security response processes are aligned and integrated, as a way to address this and to be more effective in an integrated response to different events.
14	HBR	(Groysberg & Cheng, 2017)	Board, Effectiveness, Awareness	D	In a survey of 2,900 Board Directors globally, only 8% see cybersecurity as a strategic threat; in a survey of 5,000 Board Directors of the 23 key processes for Boards, cybersecurity rated the lowest, with only 24% rating their cybersecurity processes as 'effective' or 'above average'.
15	HBR	(McNulty et al., 2007)	Breach, Response	D	Outlines a fictional (but realistic) scenario of a breach and how this was handled by executives and Board. It then explains that whilst most executives have the know-how to manage operational incidents like floods and fires, they do not have the skills or the ability to manage cybersecurity.
16	HBR	(Parenty & Domet, 2019)	Board, Risk, Critical Business Activities, Participation	D	States that companies do not manage or understand cybersecurity risk, as IT specialists focus on vulnerabilities, systems, and attacks. Tech jargon dominates this discussion, and executives and Boards cannot meaningfully participate. Provides an approach to identify critical business activities, their risks, the supporting systems' vulnerabilities, and potential attackers. Leaders and staff can be part of this, and

	Source	Reference	Key concepts represented	Relevance - D – Direct, or I – Indirect	Insights synthesised from narrative
					then responsibility for cybersecurity shifts to senior execs and the Board. Positions the responsibility for cybersecurity with the Board.
17	HBR	(Winnefeld Jr et al., 2015)	Breaches, Risk, Quality, Principles	D	Defines an approach to instil greater quality in the culture and operations in order to reduce human error that can often lead to cybersecurity issues.
18	HBR	(Pearlson & Novaes Neto, 2022)	Board, Accountability, Questions, Investment, Incident Response, Resiliency	D	Following a survey of Board Directors, offers insights on the limited nature of maturity in cybersecurity in Boards. Only 68% of respondents regularly discussed cybersecurity, and 9% said their Board did not discuss this at all. Offers 5 principles that directors should understand. 7 questions are posed as areas the Board should ensure are answered by management (important assets, protection in place, detection of breach, response plans, role in response, business recovery plans, investment levels).
19	McKinsey	(Bailey et al., 2020)	Risk, Sub Committees, Strategy	D	Discusses how leading Boards in financial services are now more active in managing cybersecurity risk. This includes setting up sub-committees, more frequent discussion of cybersecurity risks, and a more integrated cybersecurity strategy, and security metrics that measure inputs and outputs (e.g. % of environment they expect to be covered and reported on).
20	McKinsey	(Bailey et al., 2014)	Board, Reporting, Culture, Leadership	D	Posits that cyber is a leadership/CEO matter. The risk of cyberattacks span functions and business units, companies, and customers. Given the risks and large consequences, making necessary decisions can only be achieved with active engagement from the CEO and other members of the senior-management team. Suggests four areas of focus for CXOs; actively engaging in strategic decision making, driving consideration of cybersecurity implications across business functions, pushing changes in user behaviour, and ensuring effective governance and reporting is in place.
21	McKinsey	(Boehm et al., 2019)	Risk Management, Critical Activities, Critical Assets, Maturity	D	Posits that a risk-based approach to governing cybersecurity produces a more optimal and cost-effective approach that is also more effective in risk reduction. Six steps to identify the key activities and assets requiring protection, and then targeting these in context of the threat actors relevant to them. Moving from maturity based to risk-based cybersecurity.
22	McKinsey	(Lund & Richter, 2021)	Board, Education, Skills, Risk-based	D	Interview style paper with key industry subject matter experts. Highlights the importance now beyond regulated industries of cybersecurity. Posits that maturity-based cybersecurity programs

	Source	Reference	Key concepts represented	Relevance - D – Direct, or I – Indirect	Insights synthesised from narrative
					only increase controls and costs, but not necessarily reducing risk. A more targeted approach to identifying what assets (people, processes, systems) need protection is more effective and efficient.

Table 23: Candidate articles and papers from industry sources

The 43 concepts synthesised from the 22 candidate papers using GT techniques are depicted in Table 24 where the top five concepts, (in terms of occurrences and percentage of all concepts), include Board, Risk Management, Executive, Metrics, and Questions.

Concept in Literature from Industry Sources	#Occurrences in Industry Literature	% of all Industry Literature Concepts
Board	14	17.07
Risk Management	6	7.32
Executive	4	4.88
Metrics	4	4.88
Questions	4	4.88
Breach	3	3.66
Outcome Metrics	3	3.66
Reporting	3	3.66
Assurance	2	2.44
Critical Activities	2	2.44
Decisions	2	2.44
Investment	2	2.44
Resilience	2	2.44
Response	2	2.44
Accountability	1	1.22
Awareness	1	1.22
Benefit	1	1.22
Business	1	1.22
Business Decisions	1	1.22
Business Drivers	1	1.22
Business Value	1	1.22
Confidence	1	1.22
Continuity	1	1.22
Cost	1	1.22
Critical Assets	1	1.22
Culture	1	1.22
Cyberattack	1	1.22
Education	1	1.22
Effectiveness	1	1.22
Incident	1	1.22
Incident Response	1	1.22

Concept in Literature from Industry Sources	#Occurrences in Industry Literature	% of all Industry Literature Concepts
Leadership	1	1.22
Maturity	1	1.22
Participation	1	1.22
Performance	1	1.22
Pitfalls	1	1.22
Principles	1	1.22
Protection	1	1.22
Quality	1	1.22
Risk Appetite	1	1.22
Skills	1	1.22
Strategy	1	1.22
Sub Committees	1	1.22

Table 24: Occurrences of concepts in industry literature

3.4 Synthesis and Insights

There are a large number of papers on cybersecurity (3,928 and 1,001 across academic and industry sources, respectively) that match the primary and secondary search terms in Table 17 prior to any filtering. The final candidate set of papers following skimming, deduplicating, and reading is only 64 (with 42 being directly relevant), and a further 22 are identified from reputable industry sources (all of which were directly relevant). In the combined set of 86 papers, there are 64 that are directly relevant to the problem/research statement, with the remaining being indirectly relevant (but still informative). The results from the literature view, in terms of the number of papers against each of the stages, are illustrated in Figure 17.

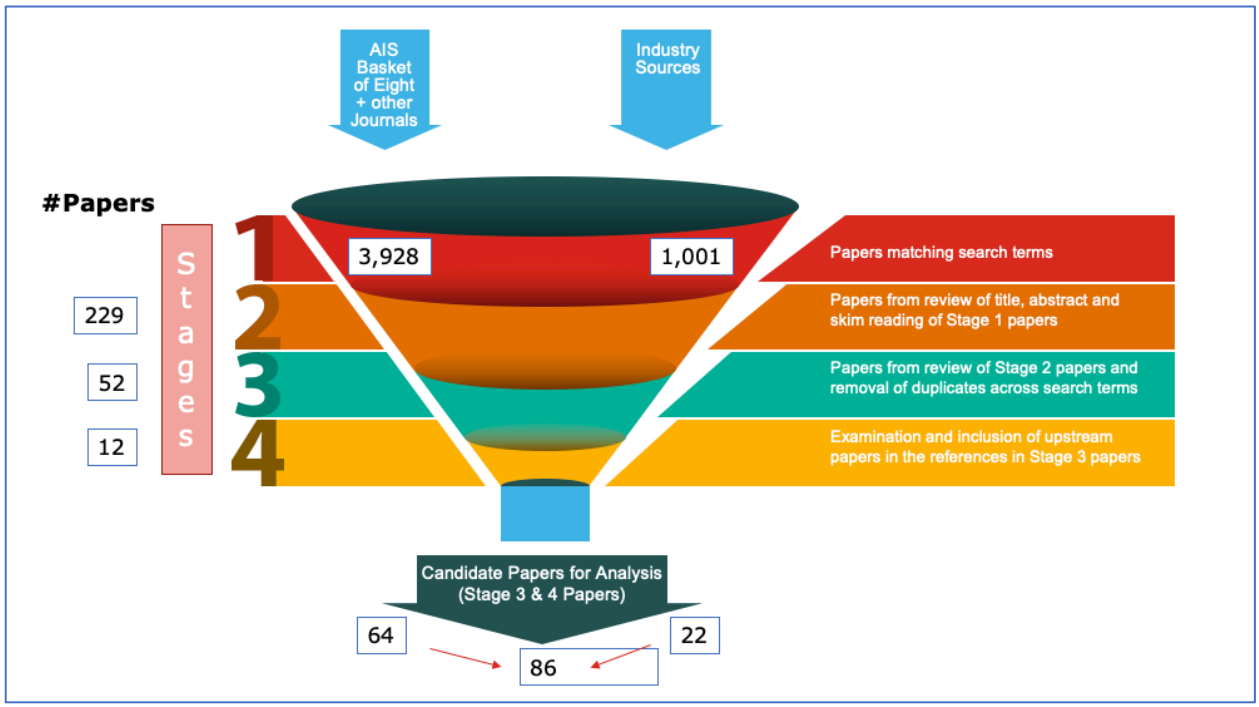

Figure 17: Summary results of literature review

The source of concepts across academic and industry papers is shown in Figure 18, including concepts that are common across both sources.

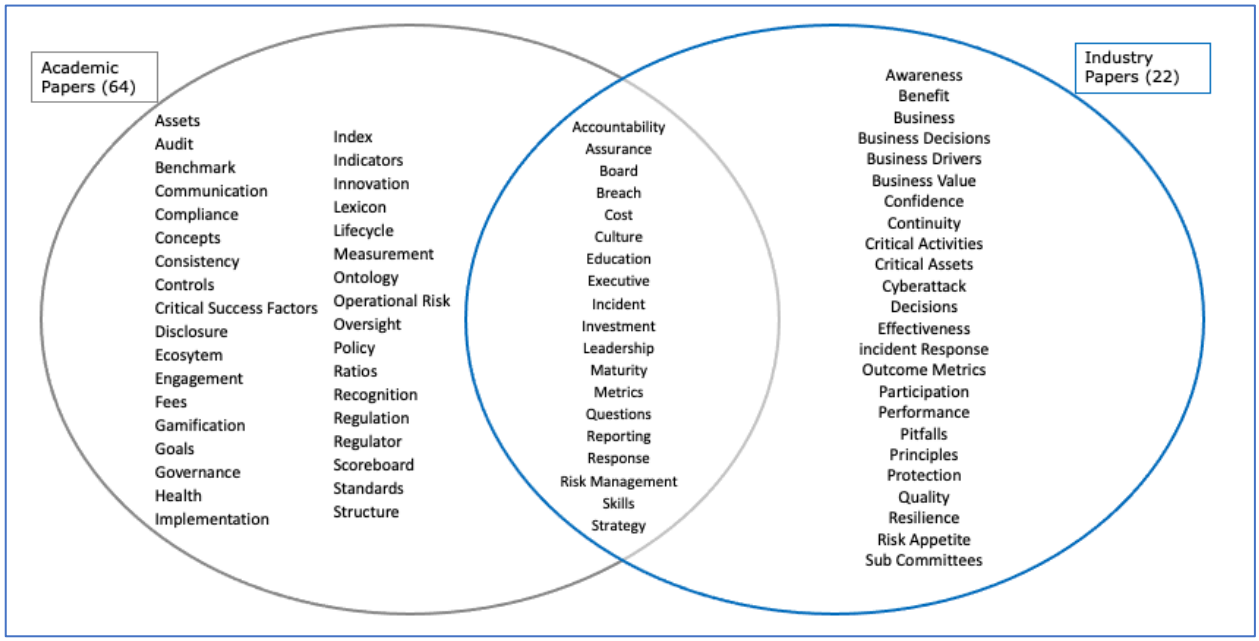

Figure 18: Concepts synthesised from academic and industry papers

The cybersecurity dimensions provided in Table 15 (section 3.2.4) are used to depict the extent of coverage in the 86 literature and industry/business sources collectively. This is shown in Table 25. The extent of coverage is classified to show the magnitude across each dimension.

	Cybersecurity Dimension	**Extent of coverage** High (H): >= 50% papers, Medium (M): 39-49%, Low (L): < 39%	**Insights synthesised**
1	Leadership	H	Literature has an abundance of coverage on principle level guidance for the NED and CXO stakeholders. However, coverage on how they govern or implement this guidance is limited. Cybersecurity culture, accountability across NED/CXOs, and reporting constructs, and committee structures have sound coverage.
2	Assurance	L	Some coverage of the need to classify assets into importance so that there is a fit-for-purpose approach to cybersecurity. There is limited coverage on how NEDs can track the health and maturity of cybersecurity at a Board level, and the breadth and depth of assurance they should seek from management.
3.	Benchmarking	L	Internal benchmarking across divisions of a company for the purposes of encouraging compliance through gamification is a common theme. However, guidance on identifying the right metrics to aid benchmarking against external benchmarks, industry standards and frameworks is limited.
4.	Terminology	L	Very limited coverage on ways to help NEDs/CXOs understand the terminology of cybersecurity, including which concepts they should learn about. There is an attempt by some authors to use lexicon maps for this through the use of a series of hierarchies to define core concepts to be covered in reporting.
5.	Stakeholders	H	Literature has been targeted at stakeholders that implement cybersecurity, including CIO/CISO/CRO and related subject matter experts in risk and security. NEDs and CXOs have very little coverage. The concept of people being the weakest link is referenced in the importance of culture, but this does not extend out to third-party risk in people or processes, including the customer impacts.
6.	Regulation	M	The evolving nature of regulation and regulators has coverage in the breadth of compliance requirements. These often build on industry standards and frameworks by mandating industry specific requirements in sectors such as banking, payments, utilities and government.

Table 25: Cybersecurity dimension coverage in final candidate papers

Table 20 (academic sources) and Table 23 (industry sources) provide a synthesis of the final results from the literature review and Table 25 covers the extent of papers overall within each cybersecurity dimension. The following sections further provide detailed discussion under each of these six dimensions, including the insights that are relevant for a Board stakeholder group.

3.4.1 Leadership

There is a consistent view in the literature on the need for Boards to hold the highest level of cybersecurity accountability across an organization in a range of facets (AICD, 2022a; AICPA, 2018; Anderson et al., 2017; Brown et al., 2017; CAQ, 2018; Dupont et al., 2023; Peppard et al., 2023; Proudfoot et al., 2023; Slapničar et al., 2023), such as establishing the strategy, setting the risk appetite, deciding on the tone of the culture, establishing principles of governance, setting roles/responsibilities, making assurance assessments, participating in desk-top exercises, reporting and adoption of standards relevant to the organization. A range of sources suggest the use of a Board sub-committee that has the skills and knowledge to discharge these accountabilities as one way to build capability in the Board and to drive cybersecurity (Higgs et al., 2016; Nolan & McFarlan, 2005). In this context, McKinsey (Bailey et al., 2020), argues the use of sub-committees, which are have more time allocated to specific topics, can allow more time to understand and govern cybersecurity matters than the relative lower frequency of Board meetings themselves. Gartner (Olyaei et al., 2021) also asserts that Boards see cybersecurity as the top source of risk and as such, should ensure they can exercise their accountability with the right skills themselves, and ensure reporting into them engages in the right language. Another aspect of accountability as suggested by (Bailey et al., 2014; Haislip et al., 2021), is that the CEO and other members of the senior leadership team are all accountable for security, and not just the CIO/CISO. The authors state that to fulfil this accountability, leaders should focus on strategy, cross-business unit controls, user behaviour and then sound governance and reporting. The organizational structures also play a key role in accountability and oversight as indicated by (Liu et al., 2020). The authors state that the centralised governance of IT gives a better outcome for reducing cybersecurity risk and also setting up a framework of indicators and metrics for reporting. Decentralised governance or a structure distributed across multiple divisions introduces variability in cybersecurity maturity, with additional cost and complexity. This insight is also a core factor in a study that demonstrates the costs of breaches in the USA for regulation that is unique to each state is higher than in Europe where a more centralised regulatory framework exists (Albawaba, 2017).

The focus on culture is an important dimension which is outlined in a range of papers including Rantos et al. (2012) who assert that the measurement of security awareness should be beyond the completion of training with a quiz to demonstrate completion. It posits a way of measuring the effectiveness through ongoing regular engagement given people are often seen as the weakest link in security. In addition, in HBR, Winnefeld Jr et al. (2015) offers a similar approach to increase the effectiveness of culture initiatives through incentives and recognition. This is also posited by Baxter et al. (2016) where the use of gamification practices (e.g. use of a leaderboard) are suggested as a way improve awareness and culture. Such practices have proven to be successful in a study of cultural change at Verizon that was Board driven (Pearlson et al., 2022). Some noteworthy insights are presented by Donalds and Osei-Bryson (2020) in terms of stating leadership styles impact the security compliance and culture in a positive or negative way. Limited literature discusses the indicators of good cybersecurity culture and identifying the questions to ask. Insights are limited to tracking the completion rates of security awareness initiatives and ensuring regular communications and awareness campaigns are performed. In regards to security culture, Schuetz et al. (2020) emphasises that that elements of the Protection Motivation Theory could guide a focus on the culture by factoring in personal motivations of individuals.

Principles to guide cybersecurity governance for NED and CXO stakeholders are found in the literature across industry and academic sources. The World Economic Forum (WEF, 2021) provides six principles

that should be embedded to ensure a cyber-resilient organization. This includes viewing cybersecurity as a business enabler, aligning risk with business needs and ensuring organizational design, including Board governance, which supports cybersecurity. Similarly (CAQ, 2018), the material from the National Association of Company Directors, (Leech & Hanlon, 2017), and AICD (2022a) outline five principles Boards should consider as they seek to enhance their capability in providing cybersecurity oversight. This includes questions that should be asked for cybersecurity assurance. These questions are grouped to target the various actors involved in this process, including Auditors, Management and Directors. Furthermore CII (2016) poses five questions to ask in order to understand the cybersecurity strategy, where weaknesses may exist, and then target investment in an informed manner.

Whilst the literature covers what Board Directors should focus on from a leadership perspective, the literature falls short of explaining how this can be discharged with the right frameworks and models. An example of this is the need for the Board to establish a cybersecurity risk appetite statement (AICD, 2022a; Anderson et al., 2017; Peppard et al., 2023; Proudfoot et al., 2023). The importance of this is argued well, in terms of being clear as a Board, that having zero cybersecurity incidents is not achievable and therefore the need to provide CXOs clarity on what levels of cybersecurity risk is acceptable. It is also important to state the desired cybersecurity resilience level. However, the literature does not propose 'how' this can be done with the right model or approach. This gap then relies on Boards having the right expertise themselves to make informed decisions off the back of management recommendations. The linkage to the overarching Board Risk Appetite Statement (RAS) and other risk management processes is also not drawn out in literature and this leaves cybersecurity risk management as a standalone domain which is undesirable from a Board governance perspective (AICD, 2022a).

3.4.2 Assurance

The Board of Directors ultimately carries legal liability for the organization it governs. This relates to not just the fiduciary responsibilities outlined in company law but also the operational risk aspects such as cybersecurity risk. As outlined in Chapter 2, regulators such as ASIC and APRA have imposed fines on companies and individuals for poor cybersecurity governance. This landscape places importance on the approach NEDs takes to attain insightful assurance that is accurate and timely. An important part of assurance is determining which assets to protect and then establishing assurance mechanisms such as accountabilities, reporting, risk assessments and audits on this scope (AICD, 2022a; AICPA, 2018; CAQ, 2018; CII, 2016). This is described in detail in McKinsey by Boehm et al. (2019) where the authors detail the importance to commence with a focus on identifying and agreeing on the assets that require protection. These assets can include business processes, systems enabling them, or even specific data. It is argued that such an approach is risk-based and allows the governance of cybersecurity in a more cost-effective manner. This concept in industry and business is termed as identifying the "crown jewels" to be protected, and then ensuring this scope attracts the management attention ahead of other areas in a targeted way. The literature is limited in providing guidance on how these assets can be identified and the dimensions of risk to consider. The steps and approach to identify these need to be detailed further for NEDs and CXO in context of cybersecurity and the set of interconnected processes and systems in today's digital landscape.

Following on from an identification of the critical assets, the nature of assurance reporting required to enable Board accountability becomes very relevant. From an audit perspective, AICPA (2018) outlines a simple reporting framework into control effectiveness and also includes an independent practitioner viewpoint as a way of seeking assurance from management. The Ponemone framework is used by Banker and Feng (2019) to classify security maturity and breaches across three areas (system deficiency, criminal fraud, and human error). Root cause reporting (in relation to cybersecurity incidents) also carries some importance in Cheong et al. (2021) which outlines the format of a reporting to regulators such as SEC, and disclosure reporting from management to Boards. These references provide a high-level view of the nature of reporting frameworks. However, they lack guidance across the security

lifecycle, and also are limited in outlining the breadth of data required. The use of lead indicators and those that are aligned to business outcomes or critical business assets (processes, data and systems) are limited and Boards struggle in this important area (Proctor, 2021b). Gartner's Scholtz (2021) also states that security presentations and reports do not resonate with senior executives and are rarely aligned to business drivers. Further to this, Proctor (2020, p. 2) from Gartner also states that in its assessments of hundreds of metrics programs annually, "almost none of these organizations are effectively measuring and reporting outcomes". Some literature (Payne, 2006), does frame basic attributes of security metrics to assist with effective reporting, including some of the characteristics that are desirable, e.g. SMART – Specific, Measurable, Attainable, Repeatable and Time-dependent. In a similar manner, Mandy et al. (2021) from Gartner outline an approach based on the CARE framework which guides defining metrics through a focus on being consistent, adequate, reasonable and effective.

Assurance on cybersecurity resilience is limited for the Board Director. This refers to the ability to recover from a cybersecurity incident in the desired time and cost parameters. This is over and above the assurance on the ability to defend a cybersecurity attack (i.e. the health of cybersecurity protection mechanisms themselves). This is a theme that has been identified by Proudfoot et al. (2023) where the authors detail the importance of Boards having focus on this in line with threats and expectations from regulators and consumers of digital services provided by the organization. For the NED, the need for assurance through risk reporting, audits, and independent reviews is seen as critical in the literature review. However, there is a distinct lack of coverage on how they can implement principle-level guidance in practice. Further, the approach to asking the right questions and having the right metrics is highlighted as a challenge, but with limited guidance on overcoming this industry imperative.

3.4.3 Benchmarking

Benchmarking or comparing aspects of the cybersecurity posture across internal divisions of an organization, or external peer organizations can be successful in driving maturity and learning through gamification practices (Baxter et al., 2016; Pearlson et al., 2022). As outlined previously under the Leadership dimension (Section 3.4.1), the authors also propose such an approach to drive the right cybersecurity culture. The approach relies on having the right metrics to compare in a leaderboard style approach and ensuring these have relevance to the stated business outcomes in an insightful way (Cram et al., 2021; Jensen et al., 2021). Other approaches to benchmarking follow a more technical route whereby a series of measurement points are defined across the protect, detect, respond and manage lifecycle (PDR-M), coupled with a calculated aggregated security index as an indicator of progress (Zhao et al., 2019; Zhuang et al., 2020). The challenge in these approaches is the selection of the right metrics that are specific, measurable, attainable, repeatable, and time-dependent (SMART), as many dashboards for benchmarking and comparison fail this quality test (Proctor, 2021b; Rantos et al., 2012). There are some interesting efforts to address this challenge in the academic literature through the use of taxonomy models that utilise a tree approach to deriving a small subset of metrics (Kormos et al., 1999; Savola, 2007, 2008). However, authors and other researchers have not extended or built on this research over the years since these papers. The inherent limitation of this approach is that the metrics and terminology are point in time, which date quickly given the evolving nature of cybersecurity and variability in the various implementation methods, as outlined in Chapter 2. A more generic approach that withstands the evolution of the cybersecurity domain is necessary to guide the selection of metrics for benchmarking and assurance. This means that practical guidance on metrics and associated lexicon that is relevant for the current industry and business context is limited for the NED or CXO. The need for guidance and frameworks to address this gap will assist in developing effective and value-adding benchmarking approaches.

A number of generic approaches are suggested in some industry literature which offer an approach of aligning cybersecurity benchmarking and metrics to business process and desired business outcomes (Buchanan et al., 2022; Mandy et al., 2021; Proctor, 2021b; Proctor & Shankel, 2023; Scholtz, 2021). This is where a common theme is to simplify metrics and focus on them being consistent, adequate,

reasonable, and effective (CARE framework). Whilst such approaches provide comprehensive support to stakeholders that design scorecards and benchmarking metrics, for the NED this does not offer a simple way of validating or conducting a litmus-test on coverage of metrics and benchmarking. Correlation to aspects such as the cybersecurity lifecycle, the extent to which metrics are leading or lagging, and ensuring the coverage in terms of depth and breadth of measures is limited. This means that in absence of such frameworks for NED stakeholders, the confidence they have in benchmarking mechanisms is lower, and as such place more reliance on CXOs and SMEs to guide them in this. A simple framework to determine the adequacy of benchmarking metrics would assist them in this regard, in a manner in which financial reporting contains key accounting measures and metrics that can be used to ascertain the financial health of an organization.

3.4.4 Terminology

The terminology that is used in the Boardroom is vastly different from the lexicon used by those that implement cybersecurity and then have to present its posture to the Board (AICD, 2022a). The challenge here is two-fold: first, the need for NEDs to educate themselves of terms and concepts (that are relevant for their governance role, in what is a rapidly evolving field that is driven by the increasing pace and complexity of the threats themselves; and second for CXOs, management and SMEs that communicate to Boards, to do so in a clear way that demystifies the topic and breaks it down into simple concepts. Whilst comprehensive cybersecurity terminology glossaries are available in standards, industry publications, and commonly available internet resources, these do not provide organizational context to the NED and require further clarification and linkage to risks impacting businesses and controls that can mitigate these. Further, as outlined in Table 11 (Research Background), the primary audience for cybersecurity artefacts are those that implement cybersecurity. The NED and CXO are least served by these as the terminology in ISO/IEC, NIST and CISM frameworks are technical in nature, and there is a lack of an approach that offers help to the NED in engaging management and subject matter experts more effectively. Papers by (Savola, 2007); Savola (2008) and Kormos et al. (1999) make use of a series of hierarchical tree structures that outline taxonomy that enables definition of cybersecurity metrics for business-level discussions. However, the use of tree structures does not extend this to a form of lexicon maps that potentially could offer two-way translation of terminology between business and technical stakeholders. More recently, Doynikova et al. (2019) identifies a series of cybersecurity management ontologies that inform the selection of appropriate security metrics covering vulnerabilities in a systems environment. The authors indicate the limitation in this due to the changing nature of cybersecurity and that to maintain the currency of such models, ongoing concepts and sources would need to be added. The evolving nature of the terminology around cybersecurity means that NEDs and CXOs would be better served by a generic approach that informs them on an appropriate education curriculum that has context of their organization and broader industry environment. This form of just-in-time education is a theme that is detailed by AlDaajeh et al. (2022) to analyse the goals of several national cybersecurity strategies. Through this, the authors propose ‘clusters’ of education in a curriculum that is aligned to the goals, risks, and solutions outlined in the strategies. This has relevance to NEDs in that a just-in-time approach such as this could narrow down areas of education and terminology to that which is relevant and timely. This would be informed by not just the business strategy in play, but also the current and emerging risks in the organization and those seen in the industry. This approach is also outlined by (Kam et al., 2022; Mehrizi et al., 2022), where the approach to terminology and education is based on embedding this into existing processes and activities of NED and CXO stakeholders, including in desk-top incident scenario exercises. Other approaches include the use of gamification to track, encourage, and recognise completion of relevant training and learning (Silic & Lowry, 2020). This is an approach to attain more success in the focus on SETA activities (security education training and awareness). From this discussion it is evident that to make terminology more easily understood across cybersecurity stakeholders is complex and challenging problem, given the changing nature of cybersecurity and the vastly different skills and capabilities seen in the Boardroom (governance) and in management (implementation). An approach that embeds such learning into regular practices and processes appears to have merit, as it enables more discussion that is timely and relevant.

3.4.5 Stakeholders

A range of stakeholders are presented in the literature when it comes to their role in cybersecurity. These include Senior Executives (CEO/CFO/CXO), SME roles such as CIO/CISO/CRO, and other staff in an organization (Banker & Feng, 2019; Evans & Price, 2020). A comprehensive study into various management roles in cybersecurity is presented by Soomro et al. (2016) where the authors identify these roles in literature. They cite the growing importance of management in cybersecurity policy, strategy, awareness, and risk assessment, with this being a key factor in managing cybersecurity risk successfully. This finding is further supported by Haislip et al. (2021) where the authors argue that the risk of a cybersecurity breach cannot be reduced by one CXO alone, and that it is a shared responsibility amongst the CEO, CFO and CIO. They go on to emphasise the importance of the CIO being part of the Senior Executive committee and playing a leadership role in cybersecurity, coupled with the role having a strong partnership with the CFO who has expertise in security compliance beyond that needed for financial control and audit. Coverage of the Board of Directors is predominantly on a principle level which gives insights into the need for them to govern and lead cybersecurity risk from the senior-most levels, as detailed in the Leadership dimension in Section 3.4.1. There is limited coverage of 'how' NEDs can implement these principles in a practical and informative manner. The limited coverage is centred on the value of Board sub-committees as a way of carving our more time and focus for this topic, and also embedding cybersecurity risk into the CEO's regular risk reporting to make use of existing processes and mechanisms (Higgs et al., 2016; Leech & Hanlon, 2017). Recent papers have provided more comprehensive insights and evidence-based recommendations through interviewing NEDs across industry and synthesising these insights. This is where Slapničar et al. (2023) suggests the extension of the 3 Lines of Accountability model to 5 Lines from the inclusion of the NED and CXO stakeholders so that they have clearer accountabilities in governance and assurance to the Board. Similarly, other recommendations suggest ways NEDs can engage a broader set of stakeholders to improve their effectiveness through, ongoing external education, desk-top exercises led by SMEs, incident response scenarios that require them to make Board level decisions, and a focus on cybersecurity resilience as part of business continuity deliberations in operational risk discussions (Gale et al., 2022; Lund & Richter, 2021; Pearlson & Novaes Neto, 2022; Proudfoot et al., 2023; Witty & Hoeck, 2022).

Increasingly, more relevant in managing cybersecurity risk is third-party risk, which includes the stakeholders that provide business and technology services to support an organization (Frank et al., 2019; Olyaei & Mandy, 2022). This is where down-stream providers, if breached, could impact upstream clients in an ecosystem that is impacted collectively. Coverage of such scenarios and stakeholders in a value chain is limited in the literature, other than where regulators demand this for risk management. An example of this is detailed in APRA (2019) where the financial regulator explicitly includes third-parties to be identified and then managed in accordance with criticality and sensitivity of the information that third-party manages on behalf of the regulated entity. For the NED, this becomes a critical extension of the scope that they have to then govern, and this demands a more holistic approach to assurance and compliance of downstream entities to ensure cybersecurity resilience of their own organization. Guidance in the literature on such external stakeholders and scope is limited, even in principle form, and this is made more challenging through the variability in cybersecurity definitions, standards and frameworks across industry as detailed in Chapter 2.

3.4.6 Regulation

Regulators have placed more importance on strengthening regulation targeted at cybersecurity risk management as the number and impact of breaches increases across the digital economy (Cheong et al., 2021; D'Arcy & Basoglu, 2022; Haislip et al., 2021; Peppard et al., 2023; SCC/SEC, 2023; Walton et al., 2021). Further, a number of regulators have imposed fines and commenced legal proceedings on organizations and individuals that have failed to adequately manage cybersecurity risk (APRA, 2023; ASIC, 2020). Aspects such as disclosure reporting in the event of a breach carry prescribed parameters from many regulators. These requirements have been supported by the literature that suggests ways to

improve the quality and timing of such disclosures through improved governance and internal culture (Cheong et al., 2021; D'Arcy & Basoglu, 2022). Regulators (and relevant professional bodies for Auditors and Accountants) have also commenced a more direct focus on stating that the Board of Directors should have the right skills mix in being able to manage cybersecurity risk (AICPA, 2018; APRA, 2019; CAQ, 2018; NACD, 2020; SCC/SEC, 2023). This more directive approach is a testament to the risk carried in the economy and the impact breaches result in for consumers, as seen recently in (OPTUS, 2023).

Whilst regulation is clear on minimum cybersecurity guidelines and standards, for example (FISMA, 2014), which applies to US government information and operations), there is limited guidance beyond this (Lee et al., 2016). The large number of standards and cybersecurity implementation methods means the choice is difficult for the NED and CXO, as outlined in Chapter 2. Guidance to the NED is limited in regard to how they should go about choosing which standard or method they should adopt, and how the choice may align to the business strategy and risk appetite statement of the organization. Standards are aimed at the cybersecurity or risk professional as detailed in Section 2.5.1 (Cybersecurity standards) and Section 2.5.2 (Target Audience). The difficulty in choice of cybersecurity standards and implementation methods manifests in complex compliance requirements and process when multiple standards or a hybrid of these is chosen (Lee et al., 2016). The authors argue that "security standards do not regulate all possible security controls", with the example of PCI-DSS standard not regulating the security of internal communication within a firm. As such multiple standards and controls emerge, resulting in a level of compliance and reporting complexity in controls. Such scenarios are an example of the challenge NEDs face when reviewing and setting the cybersecurity strategy in their governance role. Literature is limited in providing practical and implementable advice in this regard.

3.5 Implications

The literature review confirmed that cybersecurity is seen as an important and challenging matter for Boards. It also identified that the focus and coverage of literature is at a principle level for NEDs and CXOs. There is limited practical and concrete guidance on how to implement the principles and intent in literature. Further, the review confirms that the problem statement is real in industry, and appropriate research, conducted with academic rigour that is aligned to a real-life industry problem statement, would be of a novel nature and fill a gap currently seen. It is also recognised that cybersecurity is a complex and changing domain for the Board Director, and that any response in terms of a practical implementation framework, would need to be adaptable over time as this domain evolves further. In addition, the framework would need to be flexible to accommodate different governance and risk management approaches in organizations. This variability is critical given many regulators and governments promote a fit-for-purpose approach to risk management, commensurate with an organization's size, complexity and adopted risk profile.

3.6 Summary

This chapter outlined the literature review conducted to identify prior work, and the extent to which it informed the research by providing input or a starting point for the proposed framework for NEDs and CXOs. This included the methods used for the literature review and key findings. Of note was the limited number of papers that informed the research question, with only 86 academic and industry papers being identified from an initial group of 4,929 papers (3,928 and 1,001 across academic and industry sources respectively). Of these 86 papers, only 64 were directly relevant for informing the RQ to determine what framework should be developed to help non-technical audiences such as Board Directors and Senior Executives better govern cybersecurity. The concepts in these 64 papers provided some interesting insights with existing coverage largely centred on the importance of concepts such as, Governance, Risk Management, Questions, Reporting and Metrics. These insights were useful in informing the depth and breadth of the foundational models in the BCGF, and what elements were not being covered in prior literature (such as identifying which assets to protect and setting the Risk Appetite Statement in cybersecurity terms). The next chapter outlines the research methods available to

answer the research question outlined in Section 2.7, and why Design Science Research (DSR), augmented with GT techniques was chosen as the preferred method. It also covers associated methods for, ethics approval, selection of interview participants, stages of validating the research through interviews, an expert workshop, and an online survey.

4 Research Method

4.1 Introduction

The previous chapter provided an outline of the literature review conducted to examine academic and industry sources for prior work on cybersecurity governance related to NEDs and CXOs. This chapter outlines the research methods available to address the research question outlined in Section 2.7, and why DSR and augmentation with GT techniques was chosen as the preferred method. It also covers methods for ethics approval, the selection of interview participants, the stages of validating the research through interviews, an expert workshop, and an online survey.

4.2 Objective

The overarching aim of the research is to address the RQ to determine what framework should be developed to help non-technical audiences such as Board Directors and Senior Executives better govern cybersecurity. The method for this research needs to rely upon academic rigour and also ensure relevant industry experts are engaged given the limited nature of prior literature (Kothari, 2004; Vom Brocke et al., 2020). Based on these objectives, qualitative research techniques are appropriate as, if used correctly, they allow rigour in research process, and enable practical and theoretical constructs to be balanced (Fernandez et al., 2002).

4.3 Available Methods

Several qualitative research methods are now examined to determine if they can assist in the research to address the problem statement and answer the RQ outlined in Chapter 2 to determine the framework to help non-technical audiences better govern cybersecurity.

4.3.1 Grounded Theory Research

Grounded theory (GT) research is an approach that utilises qualitative techniques to systematically analyse data and formulate new theoretical constructs (Glaser & Strauss, 1967). It has application in studying individuals or groups whilst they go about the specific task at hand and then conducting interviews, observations, and collating data. This process is often repeated to support new theoretical constructs and concepts via inductive means. Four distinctive characteristics describe the grounded theory method (Urquhart et al., 2010):

- The method is theory building.
- Preconceived ideas from experts are not used to preformulate a hypothesis.
- Analysis and synthesis are repeated to generate comparison points.
- Slices of data are used to inform sampling.

Used alone, GT techniques would not enable the objectives of the research to be achieved in engaging subject matter experts and formulating artefacts that have a basis on expert review and refinement. However, when used in conjunction with other techniques, such as DSR, grounded theory techniques can complement and enhance the rigour in research (Fernandez et al., 2002). For instance, this research used GT techniques to extract key concepts from the literature selected for this research, as outlined in Chapter 3. GT techniques also play a critical role in the artefact design and validation stages.

4.3.2 Case Study Research

The case study research method has an approach of performing detailed analysis of prior studies or research with a view to synthesizing insights and findings to generate or test a hypothesis (Benbasat et

al., 1987). It has its origins in social sciences though more recently, it has been applied to information systems (Flyvbjerg, 2006). The availability of cases with associated data allows a deeper analysis of trends, gaps, and commonalities. A common criticism of case study research is that its validity is based on having a large number of cases from which to glean insights and in many instances, newer problem statements do not have sufficient history of cases upon which to base sound findings upon (Orlikowski & Baroudi, 1991). For the purposes of research into the stated problem and questions (sections 2.7 and 2.8), this method was not seen appropriate given the smaller number of cases available in areas related to NED and CXO governance of cybersecurity (Bassey, 1999; Gummesson, 2000). There is no one exemplar case that can inform the research question and the insights from cases identified in the literature review (Chapter 3) are limited and do not enable the research question to be answered sufficiently through this method.

4.3.3 Design Research

Design research (DR) is a broad field of study in the design process and method itself, across all fields or disciplines; it is not targeted per se at information systems and pre-dates the literature on DSR (Vaishnavi & Kuechler, 2015). The terminology has incorrectly been used interchangeably with other research methods. There is a level of confusion on its distinction from DSR which has the unique defining feature of learning through building artefacts (Deng & Ji, 2018; Vijay & Kuechler, 2021). Since its early inception, DR now finds researchers have added 'science' to distinguish DR being research about design, and DSR being about using design as a research method or technique for all design fields (Hevner et al., 2004). Given these insights, it is not seen as comprehensive enough to aid the research process for the problem statement.

4.3.4 Design Science Research

DSR extends human and organizational capabilities by creating new innovative artefacts to solve a problem domain (Hevner et al., 2004). It aims to create innovations that define ideas, practices, and capabilities through which the management and use of information systems can be more effectively accomplished (Hevner & Chatterjee, 2010). DSR considers design as a process (set of activities) and a product (artefact). This is explained by Walls et al. (1992, p. 7) as a verb and a noun; this is where the authors articulate design as having two dimensions, "one dealing with the product and one dealing with the process of design". The importance of rigour in the process of DSR is a key aspect detailed by Hevner et al. (2004) where the core research process is broken down into two parts, the Develop/Build of artefacts and then a phase to Justify/Evaluate these. Within these phases a range of constructs, such theories, interviews, and data analysis inform the artefacts. Seven guidelines provide direction to ensure an efficient and effective design process and importantly quality outcome in the artefacts. These guidelines assist in framing the *problem domain*, having *rigorous* research steps in a design *search process*, identifying *purposeful artefacts* through sound *design* and *evaluation*, with clear *research contributions* into the business and research communities, as well as effective *communication* of findings to appropriate audiences. The importance of rigour in the process of DSR is a key aspect that is also detailed by Vaishnavi and Kuechler (2015) which has its basis in five process steps that focus on *awareness of the problem*, *suggestion* of artefacts to address the problem, *development* of artefacts, *evaluation* of these and then *conclusion* of the research. The process steps include knowledge contribution and circumscription of theories and knowledge in an iterative manner to refine and improve artefacts. Another more recent perspective from Vom Brocke et al. (2020) is along the same theme of rigour in design process, where the view similar to Hevner et al. (2004) is that the DSR process has two stages of design, the Build (Develop) phase and then the Evaluate (Justify) phase.
The structured nature of the DSR approach which has a focus on a sound research process and embedding quality into resultant artefacts makes this a strong fit to support the research for this study. The DSR approach has been further supplemented through the use of GT techniques to synthesise concepts found in the literature review, as detailed in Chapter 3. This has enabled the identification of important concepts that need to be explored to address the problem statement detailed in Chapter 2.

4.3.5 Action Design Research

Action design research (ADR) is a design method that is based on design research techniques, but with an intentional focus on design intervention from researchers or an organizational context during the development and evaluation phases (Sein et al., 2011). This organizational input and refinement are seen as inseparable from the design of the artefact and is seen as the 'action' or intervention refining the output. The authors propose a research method that spans four key stages, namely problem formulation, building, intervention and evaluation, reflection and learning, and formalization of learning. Six key principles underpin the way research should be conducted. This method was enhanced by Gill and Chew (2019) with the addition of an idea stage at the outset to reflect the organizational business problem that requires solving and the potential approach to this. Other derivative approaches, such as participatory action design research (PADRE), have also been formulated that require iterations of participant input from an organization (Parsons et al., 2016). To address the research problem and research questions (sections 2.7 and 2.8), ADR was not deemed appropriate due to the need to shape artefacts by an organizational intervention. The nature of Board cybersecurity governance and the formulation of the BCGF requires consideration of multiple organizations and sectors, with a broader industry and business context. Therefore, to limit the formulation to an organization would not serve the same purpose, and using this approach across multiple organizations would not be effective or efficient.

4.4 Rationale for selecting DSR

DSR was chosen as the preferred method in this research for three primary reasons: first, the rigour it brings in establishing a sound process across two phases of research focussed on design and then evaluation; second, the focus on design quality through guidelines and an iterative approach to refine artefacts during evaluation; and third, the opportunity to inform artefacts through relevant theories and subject matter experts during the evaluation, and through this enable a test-and-improve approach that enhances the solution to address the problem domain. GT techniques have been applied to augment DSR. This has been needed to analyse and synthesise concepts in the literature review (Chapter 3) and in the results and evaluation (Chapter 6). This approach further strengthened the design and evaluation of the artefacts through interviews, synthesis, and quantitative evaluation.

4.5 Application of DSR

The application of the DSR framework to this body of research is depicted in Figure 19. This diagram combines elements in the framework outlined by (Hevner et al., 2004; Vaishnavi & Kuechler, 2008; Vaishnavi & Kuechler, 2015), and adapts the concepts to support the problem statement outlined in Chapter 2. Also shown in this diagram are the points at which the 7 DSR guidelines, as per (Hevner et al., 2004), are applied to ensure rigour is built into the research process.

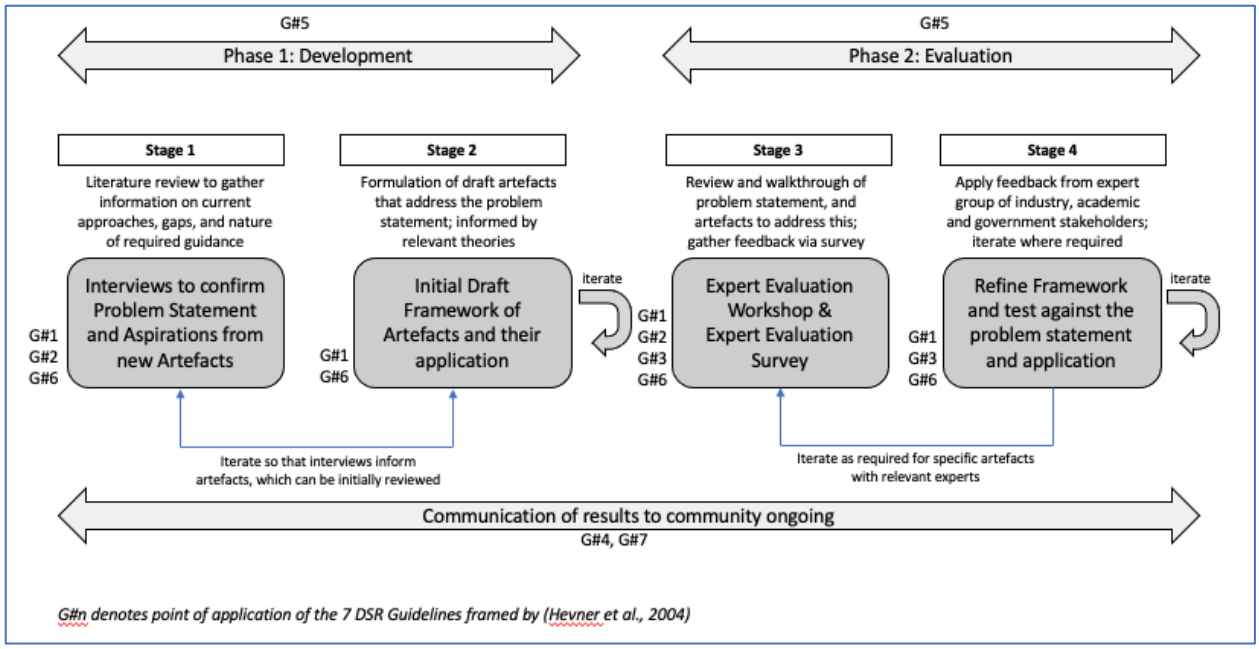

Figure 19: Design science framework and embedding of guidelines

The 7 DSR guidelines are detailed in Table 26.

Guideline Number	Guideline	Description
Guideline 1 (G#1)	Design as an Artifact	Design science research must produce viable artifacts in the form of a construct, model, a method, or an instantiation of these.
Guideline 2 (G#2)	Problem Relevance	The objective of design science research in information systems is to develop technology-based solutions to important and relevant business problems.
Guideline 3 (G#3)	Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
Guideline 4 (G#4)	Research Contributions	Effective design science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
Guideline 5 (G#5)	Research Rigor	Relies on the application of rigorous methods in both the construction and evaluation of the design artifact.
Guideline 6 (G#6)	Design as a Search Process	The search for an effective artifact requires utilizing available means to reach the desired ends while satisfying laws in the problem environment.
Guideline 7 (G#7)	Communication of Research	Design science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Table 26: DSR guidelines as per (Hevner et al., 2004)

Further detail on the implementation of each of the 7 DSR guidelines into the chosen research method depicted in Figure 19 is provided in the following sub-sections. This also includes augmenting this approach with GT techniques to enhance the rigour of the data analysis and the traceability of artefacts to essential components of the problem statement.

4.5.1 Guideline 1 (G#1)

Requirement – Design as an Artefact

This guideline informs the construction of artefacts that are viable and are in the form of a construct, model, method, or instantiation. These artefacts define ideas, practices, capabilities, or products through which the analysis, design and operations of information systems can be effectively achieved.

Implementation

At the outset in the research process defined in Figure 19 (Phase 1, Stage 1), an initial literature review was conducted to provide informed context to the problem statement and identify prior work that had

been carried out. GT techniques were used to identify concepts in the literature that detail the challenges for NED and CXO stakeholders. The review and synthesis informed a draft set of artefacts that could be used as a discussion point in the research. Following this, experienced participants were interviewed to collect their pain points and aspirations regarding cybersecurity governance at a Board level. This also included a level of direction on emerging draft artefacts. This process helped to inform and refine the problem statement, which is detailed in Chapter 2. Further, the interviews informed the extent of gaps, best practices, and unmet needs that require fulfillment through new or adapted artefacts. The artefacts discussed included standards, frameworks, models, and techniques used by NEDs. A more current literature review (detailed in Chapter 3) further informed this work through the synthesis of academic and industry papers using GT techniques that provided deeper analysis of the needs and potential artefacts to meet the needs. Table 27 summarises the implementation steps taken to meet Guideline 1.

Step	Research Aim	Description	Outputs
1	Inform & Design	Initial literature review of prior academic and industry papers, with synthesis of challenges and draft artefacts	Draft artefacts and proposed questions for interviews
2	Inform	Expert interviews to collect pain points and aspirations in Board-level cybersecurity governance	Refined draft artefacts and synthesis of gaps as seen by NEDs
3	Inform	Final literature review of prior academic and industry papers, with synthesis of concepts and approaches	Comprehensive synthesis of prior work, gaps, and problem statement
4	Design	Using initial draft artefacts and interview feedback, produce draft version of framework	Draft framework, models, and usage scenarios
5	Evaluate	Expert evaluation workshop with industry wide experts to review the draft Framework	Refinements and improvements to draft framework
6	Evaluate	Expert evaluation survey conducted online with industry-wide experts	Further feedback to refine and improve framework

Table 27: Steps taken to implement guideline 1

4.5.2 Guideline 2 (G#2)

Requirement – Problem Relevance

This guideline places importance on having a sound business problem to address and solve, as it relates to the management and use of information systems. Central to this is understanding the challenges in the current state and the desired future state.

Implementation

The relevance of the problem is grounded in rigor starting from an initial literature review that then was expanded upon to explain the business challenges presented and the gaps in the prior work. This is detailed in Chapter 2 and covers the conceptual background and the challenges faced by cybersecurity governance by NEDs. The detailed literature review in Phase 1/Stage 1 of the academic and industry sources, as outlined in Chapter 3, informed the challenges and coverage in prior artefacts and approaches. This was further enhanced using the participant interviews which included experienced experts in NED/CIO/CISO roles in industry. The interviews identified the current pain points that result in challenges in governing at a Board level, and the aspirations participants have in addressing these. Through this phased approach, the problem statement and its relevance were detailed.

4.5.3 Guideline 3 (G#3)

Requirement – Design Evaluation

The quality of the evaluation of the design artefact is the focus for this guideline to ensure that there are rigorous methods to conduct this. This is critical given the role the artefacts need to play in addressing the problem in Guideline 2.

Implementation

This guideline is addressed in Phase1/Stage 2, where initial draft artefacts were informed and developed in conjunction with the participant interviews. These were progressed and enriched by the literature and theories to an initial draft version of the Board Cybersecurity Governance Framework (BCGF). Phase 2 then consists of an expert evaluation workshop (EEW), where the problem statement was confirmed, and a walkthrough of the draft framework was conducted using specific business scenarios faced by NEDs and CXOs. Feedback was sought in the workshop. The quality of the artefacts in the BCGF were evaluated by the participants in the series of steps outlined in Table 28.

Evaluation Criteria	**Workshop**		**Online**
	Evaluation Step 1	**Evaluation Step 2**	**Evaluation Step 3**
Completeness	Business Scenario Walkthrough	Workshop Feedback	Quantitative Survey
Importance	Business Scenario Walkthrough	Workshop Feedback	Quantitative Survey
Relevance	Business Scenario Walkthrough	Workshop Feedback	Quantitative Survey
Practicality	Business Scenario Walkthrough	Workshop Feedback	Quantitative Survey
Improvement Opportunities	N/A	Workshop Feedback	Quantitative Survey & Qualitative Feedback

Table 28: BCGF evaluation approach

The expert evaluation survey (EES) also allowed non-structured free-form comments for qualitative feedback, as well as structured questions to capture the BCGF components that participants would add or remove. There were 28 questions overall covering the evaluation criteria in Table 28, and as detailed in Chapter 6 - Results and Evaluation, with 19 expert participants completing the online survey. Stage 2 in Phase 1 allowed refinement of the BCGF as a consequence of the learnings from Stage 1. This approach aligns to the descriptive DSR evaluation method in Hevner et al. (2004) where informed argument and scenarios are defined mechanisms to evaluate artefacts. After applying feedback from the workshop/survey, models in the updated framework were applied to specific Boardroom presentations and presented to academic forums. This enabled further refinement to the BCGF. The BCGF has been intentionally designed to be abstract and allow a level of customisation to enable a fit-for-purpose for an organization considering its specific risk management approach and the desired level of maturity in cybersecurity posture.

4.5.4 Guideline 4 (G#4)

Requirement – Research Contributions

The application of the DSR method must provide clear outcomes, in either the form of design artefacts, design construction knowledge and/or evaluation knowledge. The artefacts must assist in solving the stated problem in whole/part and present new contributions that are implementable for users in the business environment, such as instantiating design artefacts to contribute to the business environment by solving previous problems.

Implementation

The approach defined in Figure 19 resulted in an evaluated and tested BCGF through the design (Phase 1) and validation (Phase 2) stages. The BCGF is a set of design artefacts called models, each of which are used in different business situations and scenarios by NEDs or CXOs. The models also have a clear

purpose, inputs, outputs, and usage guidelines to aid the instantiation of these in the business world. These are the design artefacts, as per Guideline 4, which are outlined in Chapter 5 in detail. The unique and novel aspect of these and the suitability of these design artefacts to solve the problem faced by NEDs and CXOs (as outlined in Chapter 2, Research Problem Statement) is confirmed through two primary design steps. First, through the DSR process, the models have undergone construction, review, refinement, and validation by expert SMEs, who are seen as leaders in their field as per their expertise detailed in Appendix 8.3. In addition, these models have been shaped by learnings and insights from prior literature and theories, as outlined in the literature review in Chapter 3. Second, the feedback from the EEW and associated EES refined the artefacts to ensure they were appropriate in addressing the

problem statement in a practical and novel manner. The feedback from this is detailed in Results and Evaluation, Chapter 6. In addition, the application of the models was tested through use in real Board situations that required the assistance of NEDs, as per the engagements outlined in the section on List of Publications and Presentations. The uniqueness is confirmed through this rigorous design process by stakeholders, and practical use in industry to date. It is expected however, this framework will evolve further through use and additional focus through subsequent academic research.

4.5.5 Guideline 5 (G#5)

Requirement – Research Rigor

DSR requires the application of rigorous methods in the design and evaluation of artefacts. In the design stage, this includes a clear line of sight from the artefacts to the specific problem statements identified. It does not necessarily mean over-reliance on mathematical or theoretical proof, especially in problems where aspects related to behavioural science are important, e.g. the human element in the human-machine interface. In the evaluate stage, this is assessed by adherence to appropriate data collection and analysis techniques. These aspects are further articulated by Benbasat and Zmud (1999) who stress the importance of ensuring the relevancy of the artefacts to the problem and that these artefacts are implementable for the benefit of practitioners.

Implementation

The implementation of this guidelines traversed a range of activities across the design (Phase 1) and evaluate (Phase 2) parts of the DSR process, as shown in Figure 19. Specifically, there was a focus in Phase1/Stage 1 to ensure the problem statement for NED and CXO stakeholders was understood, and that this was verified through participant interviews. The core models of the BCGF are informed through this interaction. Further, this stage informed the problem statement through a comprehensive literature review covering academic and industry sources targeted at this stakeholder group and cybersecurity governance. This was supplemented by the application of GT techniques to ensure rigour and not just to synthesise the data to design draft artefacts, but also to use similar approaches in the validation and traceability of the final artefacts to the original pain points and aspirations of NED and CXO stakeholders. In the design phase, Phase 2/Stage 3 focused on an EEW to first confirm the problem statement, and then review the draft BCG framework in accordance with a defined analytical approach covering the completeness, importance, relevance, and practicality of the artefacts. Phase 2/Stage 4 then refined the BCGF based on this work and incorporated feedback from the application of artefacts in specific Boardroom scenarios, as per section on List of Publications and Presentations.

4.5.6 Guideline 6 (G#6)

Requirement – Design as a Search Process

The DSR process is iterative and akin to searching for artefacts that can then be implemented in the business environment to resolve the problems relevant stakeholders face. In other words, DSR is essentially a search process to discover effective and efficient solutions to a problem. This requires understanding the environment (in a design and behavioural science manner) and the laws or regulations with this. The identified artefacts need to be tested, measured for effectiveness, and include a level of abstraction that can effectively cater for the nuances in the business environment (Hevner et al., 2004).

Implementation

The DSR approach outlined in Figure 19 established key iteration points that enabled feedback on confirming the problem statement and reviews of the draft artefacts through a series of steps. This are depicted in Phase 1 across Stage 1 and Stage 2, and in Stage 2 where the EEW and EES resulted in the refinement of the artefacts. These were further enhanced through the use of the artefacts in Boardroom settings as a Senior Executive (CXO) presenting cybersecurity material, and as an NED using the artefacts

to educate and improve the governance of cybersecurity, as detailed in the section on List of Publications and Presentations.

4.5.7 Guideline 7 (G#7)

Requirement – Communication of Research

This guideline focuses on the need to communicate the research to both technology and management-oriented audiences. This offers a benefit to practitioners from the use of the artefact to assist in solving the problems they face, and a level of feedback from them to the researcher to evaluate and extend the artefact. Further, this builds a knowledge base from which the broader community can benefit in terms of the applied research process and instantiation of the artefact in industry.

Implementation

Communication of the research has been an ongoing process, as shown in Figure 19. This important activity spanned both Phase 1 and 2 and is ongoing. The formal engagement to date is detailed in the section on List of Publications and Presentations. Further engagements will be established with a view to target academic and industry forums to communicate and enable further improvement and extension of the artefacts. The nature of cybersecurity requires such open collaboration amongst stakeholders that are vested in the protection of systems and data for the modern digital economy.

4.6 Research Instruments

The DSR research process is supported by a range of steps and artefacts to ensure rigour in the approach and compliance to relevant policies and standards, outlined in the following sub-sections.

4.6.1 Data Management Plan

The Research Data Management Plan (RDMP) outlines the approach adopted to ensure good data management practices in line with UTS policies and procedures, and the Australian Code for the Responsible Conduct of Research. The RDMP was developed at the outset prior to commencing the research process and was maintained over the duration of the research. The UTS Stash system was used to store the contents as this ensures relevant information is held centrally in accordance with the requirements. The plan covers aspects such as the purposes for which any information is collected/used, how the data is captured, where the data is stored, who will have access, the data security classification and how the data will be protected.

4.6.2 Ethics Approval

The approval for conducting participant research for this study was granted by UTS in May 2022 following a comprehensive submission as per the research guidelines in the Australian Code for the Responsible Conduct of Research and the National Statement on Ethical Conduct in Human Research. The UTS Ethics Approval reference for this research is ETH22-7097, and the official letter of approval is presented in Appendix 8.2. The ethics application detailed the manner in which the research would be conducted and how stakeholders would be engaged to ensure the work was conducted in accordance with the principles of honesty, trustworthiness, respect, and accountability. This approval included the manner in which participants would be approached, provided with adequate detail to determine if they wanted to accept the invitation, and also particulars of what they should expect. For detail on the way in which engagement and consent was obtained from participants, see Appendix 8.4.1 for the specific document used. Similarly, for detail on the engagement approach for the participants of the EEW and EES, see Appendix 8.4.2. This level of rigour was followed at the outset to ensure the integrity of the research and this approach was periodically confirmed for compliance by the UTS Ethics Secretariat office.

4.6.3 Participant Profile

One-on-one interviews were conducted with 15 highly experienced participants. These participants were chosen for the breadth of their industry experience across multiple sectors, the tenure they had in terms of industry experience, and them having held the NED, CIO or CISO roles several times in their career. This ensured that highly experienced subject matter expertise, with experience in receiving or providing cybersecurity assurance to a Board of Directors, was engaged in the research. The average industry experience of the participants was 34 years and included coverage of most of the ISIC (International Standard Industry Codes) – the only ones not covered were those industries that had minimal reliance on information systems and their security, e.g. forestry and fishing. The extent of the experience brought by this cohort of participants was more important than aiming for a large number of interviewees with less experience as a whole. See Appendix 8.3 for more details on the extent of participant experience and industry coverage.

4.6.4 Consent Forms

Prior to engaging participants for the one-on-one interviews and subsequently for the EEW, consent was obtained from each individual. It was made clear to the participants that involvement was entirely optional, and that they could withdraw at any time. Further, it was made clear that only their industry and business perspective was being sought and no reference to any specific organization was necessary in the engagement and should be avoided. Copies of the consent forms can be found in Appendix 8.4.

4.6.5 Participant Questionnaires

At the outset as part of the Ethics Approval process, questionnaires were developed to outline the questions to be asked in the one-on-one interviews. These were designed for the participants who were NEDs on various Boards and accountable for the governance of cybersecurity, and CIOs/CISOs who reported to Boards on cybersecurity risk matters. The questionnaires targeted feedback on pain points, aspirations, assurance mechanisms, and free-form input into Board-level cybersecurity governance. Detail on the questions can be found in Appendix 8.5.

4.6.6 Expert Evaluation Workshop

The EEW included the 15 participants that were interviewed in the one-on-one interviews, with five additional industry experts from academic institutions, big-4 management consulting firms, institute of directors, government, and experienced NEDs. Key in this mix was the experience of this cohort from a domestic and international perspective regarding cybersecurity management. The workshop was structured as shown in Figure 20.

Figure 20: Expert evaluation workshop agenda

The context included an overview of the problem statement and the research question (Appendix 8.6). This allowed participants to collectively provide feedback and confirmation of the problem being solved and that this was an industry need that required further support. Following this, the purpose of the workshop was made clear to the participants and what was included/excluded (Appendix 8.6). This was necessary to set expectations and ensure an effective use of everyone's time. A walkthrough of the BCGF was conducted, with a focus on each of its artefacts and the scenario in which they would be applied. After this, time was allocated to seek verbal feedback on elements of the BCGF. This allowed responses to general clarifications and questions and allowed attendees to provide feedback in a general way on aspects of the framework. Finally, an online EES was conducted to seek feedback. This approach allowed more structured feedback and ensured further data could be captured on the BCGF for subsequent analysis.

4.6.7 Expert Evaluation Survey

The EES was designed and operated in the UTS Qualtrics environment. This was made available during the EEW and closed 2 days later. Most participants completed the survey during the workshop. The structure of the survey is outlined in Figure 21. This was used to enable participants to orient themselves with the survey format, and then launch via a URL or QR code.

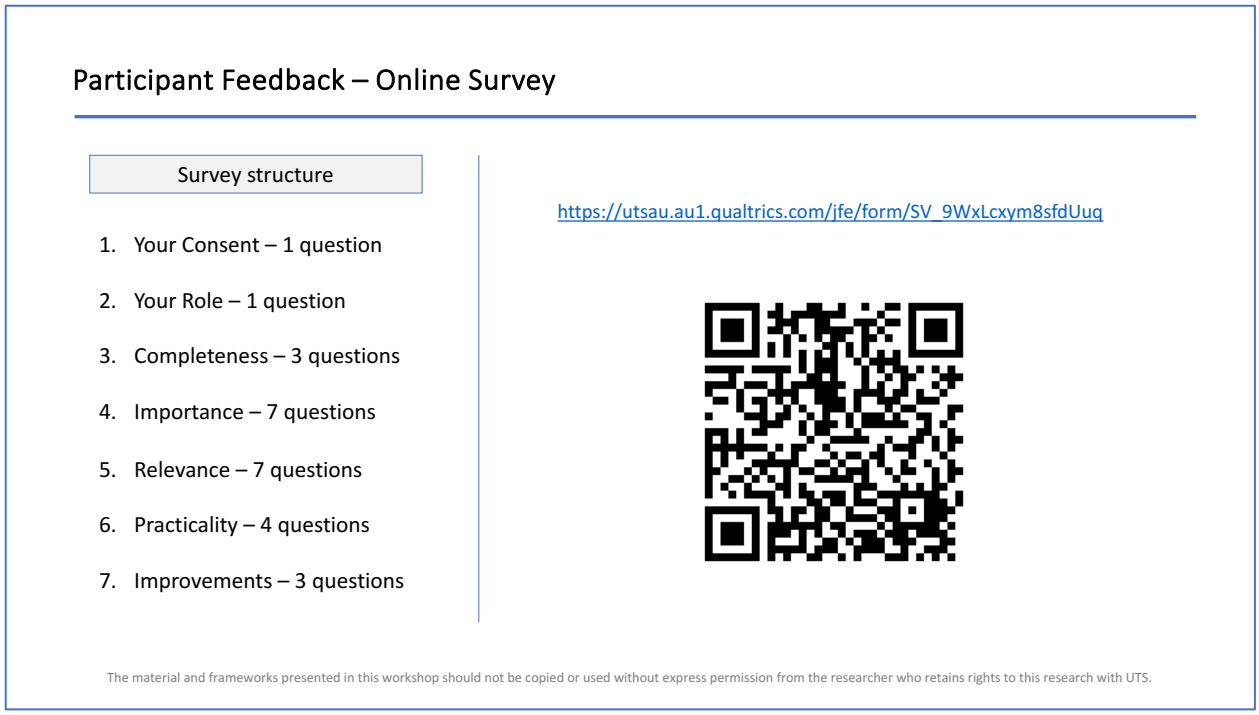

Figure 21: Expert evaluation survey structure

The consent question was presented at the outset in the questionnaire to ensure participants understood this was optional and anonymous. If consent was not given by a participant, then further questions were not presented, and the processes ended. Following consent, information on the participant's primary role was requested (either NED, CIO, CISO, Consulting & Advisory Service, Academic Research Specialist, or other). This was done to enable data analysis and distinguish any potential variation in responses per role. Questions were then presented to capture feedback on the BCGF for completeness, importance, relevance, and practicality. These were assessed on a 5-point scale (Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree). A final section to capture free-form suggestions on improvements was presented in terms of elements of the BCGF that should be removed/added or changed. Further details of the consent and survey questions are in Appendix 8.7.

4.7 Research Evaluation

The research evaluation was informed by the literature review in terms of confirming the problem statement, and then further informed by participant interviews and synthesis of the discussions. The EEW and EES were key in seeking expert review in a workshop and survey format.

4.7.1 Literature Review – Synthesis

As per the DSR method, it is important to describe the problem statement accurately upfront (section 4.5). A key aspect of this is to search for prior literature that may have examined this problem and produced an artefact that can address the need in whole or part. A comprehensive literature review of academic and industry sources was conducted to ascertain the extent to which the existing literature addresses the roles of NEDs and CXOs and outlines their pain points and aspirations. This review is detailed in Chapter 3.

4.7.2 Participant Interviews – Concepts

The participant one-on-one interviews (15 in total and conducted virtually and in-person) with experienced NEDs/CIOs/CISOs were synthesised to identify common patterns in their responses. This included mapping key terms into categories such as party, process, event, object, state, metrics, or

standards/frameworks. Such an approach to synthesis allowed the frequency of certain terms to be identified and the extent to which these are front-of-mind for the participants. These concepts informed the nature of the models required within the BCGF and the challenges these solved for Board governance of cybersecurity. This analysis is presented in Chapter 6.

4.7.3 Expert Evaluation Workshop – Usage

The EEW was conducted to walkthrough the usage of the models in Boardroom scenarios, and how the application of these would assist NEDs and CXOs in better governing the posture of cybersecurity risk. Clarifications on the aspects of the BCGF were provided where required by participants, and in the course of this, they provided initial feedback on the applicability of the BCGF in specific Board processes.

4.7.4 Expert Evaluation Survey – Evaluation Criteria

The EES was structured to capture feedback on the BCGF across several areas. These included completeness, importance, relevance, practicality, and potential improvements of the framework. Additionally, the walkthrough of the BCGF included a scenario-based approach on when each component of the framework would be used in the context of the cybersecurity lifecycle and Boardroom agenda. A description of the framework is presented in Chapter 5 and the responses from the survey are analysed and discussed in Chapter 6.

4.8 Research Validity and Limitations

The validity of the research can be described as focusing on the quality of the design process and the dependability of the research findings (Larsen et al., 2020, p. 288). Here the authors define DSR validity as "formalized procedures for justifying arguments and conclusions of a research study involving the design, development and/or evaluation of IT artifacts to solve identified problems." Others, such as Gregor and Hevner (2013) also cite validity as a research process that creates and evaluates IT artifacts intended to solve identified organizational problems. The validity of this specific research was ensured through the adoption of the rigorous and well-known DSR method, which at the outset involved identification of the research problem through a comprehensive literature review of academic and industry papers, as detailed in Chapter 3. It was important to examine both sources so that insights complimented each other, and through these, important concepts arising from different viewpoints were not overlooked. Following on from this, the research approach established a detailed process that adopted DSR and was augmented with GT techniques to synthesise the literature findings to inform the solution. The validity of the solution was attained via discussions of the problem statement and draft solution with experienced interview participants, and then a structured EEW that brought the BCGF to life by explaining the application of this in Board scenarios. Further to this, the solution (BCGF) was evaluated through an online survey to ensure the models in this were relevant, general, and applicable in a broad industry context to address the research problem. This approach of interviews, workshop and survey allowed data collection in three different ways to inform the validity of the research.

This approach to validity adopted internal and external dimensions (Larsen et al., 2020; Peffers et al., 2008). The rigour in the internal validity was attained by the use of the DSR method augmented by GT techniques to ensure the problem identification, solution design an evaluation was comprehensive. The external validity was attained by expert evaluation in interviews, workshop and online survey that brought in cross-industry and broader academic experience to review and evaluate the solution. The external dimension also included the selection of highly experienced participants, known for the roles they held, experience in Board governance, and industry expertise across multiple sectors, as detailed in Appendix 8.3 where the average industry experience of participants was 34 years.

Although the validity of the research approach was comprehensive, like any research project, this research has some limitations. The cybersecurity field is an ever changing one as outlined previously in

terms of the threats and sophistication of attacks. As such, the BCGF will require ongoing assessment on the extent to which it remains applicable for the NED and CXO roles. New risks and threat scenarios may trigger updates and refinements. Second, as the knowledge in industry grows in cybersecurity, some models in the BCGF may become redundant as such methods may well migrate into baseline education, and industry standards for the NED and CXO stakeholder group. The other limitations centre on the number of people interviewed, the number of models developed from the research, and the extent of workshops and online surveys across the broader industry. These limitations arise from the extent of engagement and duration of the research, as these aspects could have been extended to larger numbers and a longer time period. Whilst this may have yielded more support for the solution, or slight variations to the models, the ever-changing nature of the cybersecurity field would have introduced a risk arising from the currency of the problem statement and solution. Finally, the likelihood of research bias, which can arise from a strong opinion from a narrow subset of interviewees, was addressed in the evaluation workshop where opinion and discussion from various viewpoints were sought. The online evaluation survey also enabled the risk of bias to be minimised.

4.9 Summary

The quality of a research output depends on a rigorous research method. This chapter provided an outline of the research methods available to answer the research question and detail on why DSR was chosen as the preferred method. It also outlined how the 7 Guidelines seen in the DSR methods were implemented in the research process. The chapter also covered the approach taken for ethics approval, selection of interview participants, and stages of validating the research through interviews, an expert workshop, and an online survey. The core of the research method centred on a detailed literature review of prior academic and industry papers to articulate the problem statement, and then data collection and evaluation from interviews, the workshop and the online survey to capture and evaluate data. The next chapter covers a detailed outline of the BCGF that has been developed and evaluated through this research method to address the RQ to determine what framework should be developed to help non-technical audiences such as Board Directors and Senior Executives better govern cybersecurity. The chapter covers the 7 models in the BCGF and the way they can be applied or instantiated in Board cybersecurity interactions.

5 Board Cybersecurity Governance Framework (BCGF)

5.1 Introduction

The previous chapter provided an outline of the research methods available to answer the research question and provide detail on why DSR was chosen as the preferred method. It also outlined how the DSR method was adopted for this research augmented with grounded theory (GT) techniques. This chapter details the Board Cybersecurity Governance Framework (BCGF) that has been developed and evaluated through this research method. It covers the 7 models in the framework, including the purpose of these, and the way they can be instantiated in Board cybersecurity scenarios in organizations.

5.2 BCGF Development

The BCGF has been developed through a series of research stages including a detailed literature review spanning academic and industry sources, one-on-one interviews with experienced NEDs, CIOs and CISOs, reviewing and refining the findings through an expert evaluation workshop, expert evaluation survey, and supporting the findings through a theoretical viewpoint. This was outlined in Section 4.5 where the application of the DSR was detailed, along with use of GT techniques. Further, the concepts found in the literature review (shown in Figure 18, which shows the concepts synthesised from academic and industry sources and their overlaps), informed the BCGF scope. This scope is targeted for use by NEDs and CXOs throughout various stages of the cybersecurity lifecycle. Within the BCGF, 7-foundational models are outlined for this audience to apply and use in their roles to better govern the posture of cybersecurity risk. The components in the BCGF along with the usage guidelines for each foundational model are presented in this chapter.

The BCGF has been developed to address the RQ to determine what framework should be developed to help non-technical audiences such as Board Directors and Senior Executives better govern cybersecurity. The BCGF is organised into 7 foundational models which have been informed by the research method detailed in Chapter 4, which included a detailed literature review, interviews, expert evaluation workshop and expert evaluation survey. The BCGF has three important views within it (journey, stakeholder, and perspective). These views have been synthesised from cybersecurity implementation frameworks outlined in Table 7 in Section 2.3. These methods consistently raise the importance of being conscious of the stage in the cybersecurity lifecycle, the stakeholders of relevance, and whether the stakeholder perspective is to govern or implement cybersecurity. These three views are depicted in Figure 22, where the overlap or intersections of these areas is also relevant. In this diagram, intersections allow analysis and discussions that are relevant for that inter-relationship alone, or all three collectively.

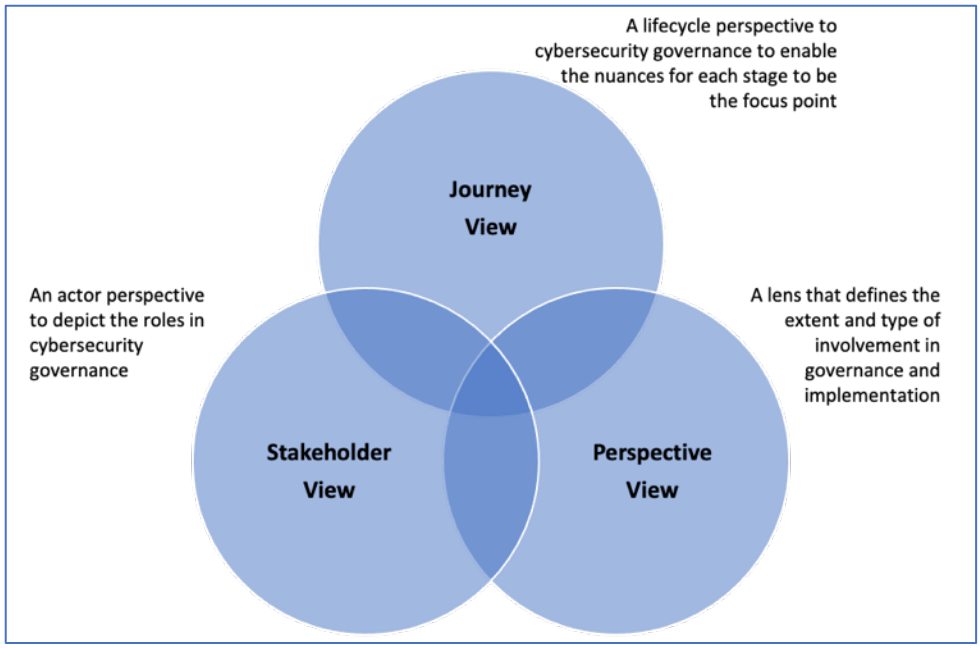

Figure 22: BCGF - core views

The intent of the three core views is described in Table 29. Such an approach allows segmentation of activities into what is relevant for a stage, stakeholder, and role. The framework then becomes more practical and applicable in different scenarios.

View	Description
Journey	A lifecycle perspective of cybersecurity governance to break the framework into practical stages to draw out nuances in activities.
Stakeholder	An actor perspective of various stakeholders involved in cybersecurity governance to ensure the series of models are fit-for-purpose for stakeholders in the lifecycle.
Perspective	A lens that defines the extent and type of involvement in the various stages of the lifecycle for each type of stakeholder.

Table 29: BCGF core views description

These views are embedded into the BCGF, which is comprised of 7 foundational models that represent key activities that are specifically relevant for NEDs and CXOs. Each model consists of meta data covering the dimensions shown in Table 30.

Model Dimension	Dimension Description
Purpose	High level overview of aspects depicted in the model and the rationale for them.
Business Scenario	The industry situation under which the model would be utilised.
Stakeholders	The stakeholders and their role in the business scenario and in adopting the model.
Overview	A broad description of the model covering the rationale for it and importance.
Inputs	Input necessary to apply the model.
Implementation Guidelines	The approach to using the model and making it fit-for-purpose and practical.
Outputs	The expected outputs from the application of the model.

Table 30: BCGF model metadata

The core views in the BCGF and its 7 foundational models are detailed in the following section.

5.3 BCGF – Core Views

5.3.1 Journey View

The journey view in the BCGF is aimed at driving a distinct focus on the different aspects of cybersecurity over defined stages in a lifecycle. These stages are akin to the approach taken in the NIST Standard (NIST, 2018) which uses them to define the focus on specific activities and controls for

cybersecurity implementation. This staged approach is also applicable in the BCGF, however, to make this more relevant to NEDs and CXOs, some refinement has been necessary (compared to the NIST lifecycle) through research and validation to focus on the governance aspects. The primary change is the first stage being termed 'Establish' – which was seen as more appropriate than the 'Identify' stage for NEDs and CXOs as a way of establishing the foundations of cybersecurity in terms of the assets to protect and set the risk appetite and standards to which to comply. Other changes include the definition of the aims and activities that are more relevant for this audience, whereas NIST is primarily concerned with activities for the cybersecurity professional and the implementation of controls. The core aims and activities for the Board are detailed in this lifecycle view in Figure 23, which states the aims for NEDs and CXOs in each stage and the activities they must conduct.

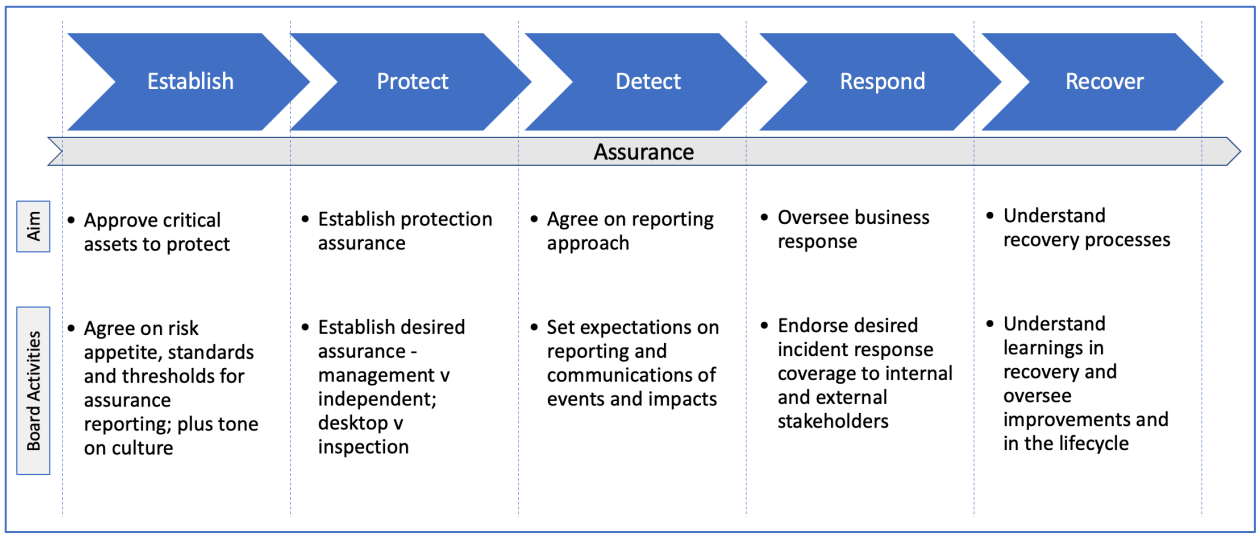

Figure 23: Journey view

5.3.2 Stakeholder View

The linkage of NEDs and CXOs to downstream stakeholders is important, including the alignment of strategies and operational imperatives between these stakeholders. This is a two-way linkage. As such, a layered approach has been taken to draw a distinction on the various roles in play, and in that context, articulate the focus of this research. These role types are represented in Figure 24 with the focus for this research being on the NED and CXO layers alone. As the literature review in Chapter 3 depicts, this stakeholder group is not well served in practical frameworks and models, beyond principles and general guidance. The focus of this research is on this cohort.

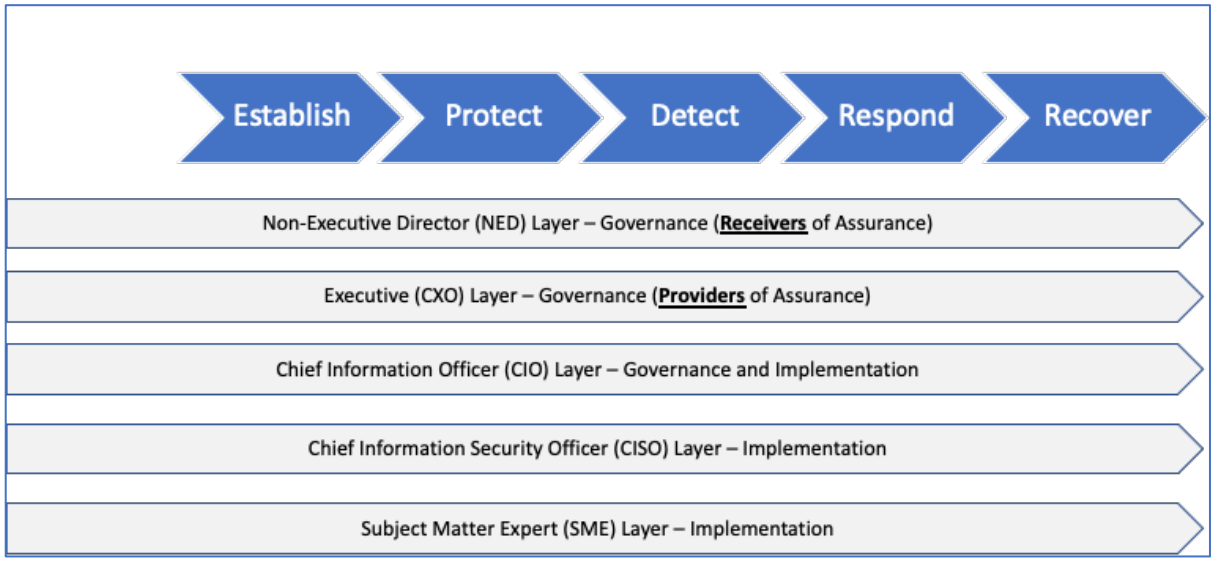

Figure 24: Stakeholder view

5.3.3 Perspective View

The perspective of each stakeholder is critical to ensure clarity in role and involvement. The upper layers in the stakeholder view have a larger role in the governance and audit of the cybersecurity posture, whilst the lower layers are focussed on implementation. Naturally, there is a cross-over in the form of dual roles in the middle. The extent of involvement is represented in Figure 25.

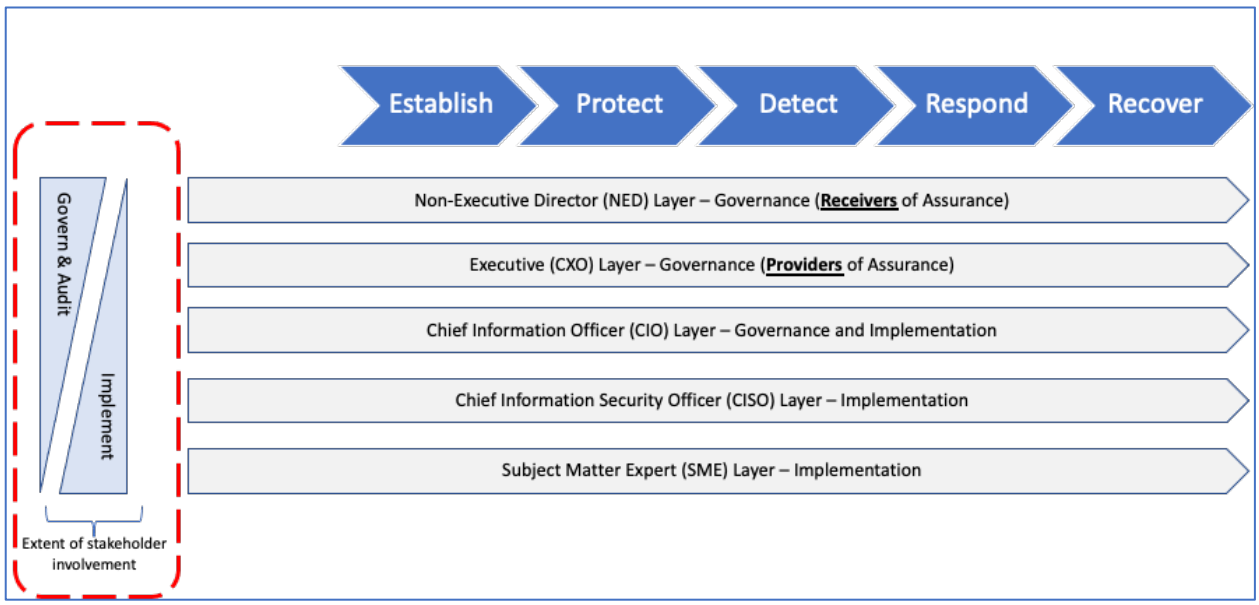

Figure 25: Perspective view

5.3.4 BCGF Overall Concepts

Figure 26 illustrates the linkages between the three core concepts in the BCGF (journey, stakeholder, and perspective views) and depicts the relationship between stages of the lifecycle and the involvement of stakeholders across cybersecurity governance and implementation accountabilities.

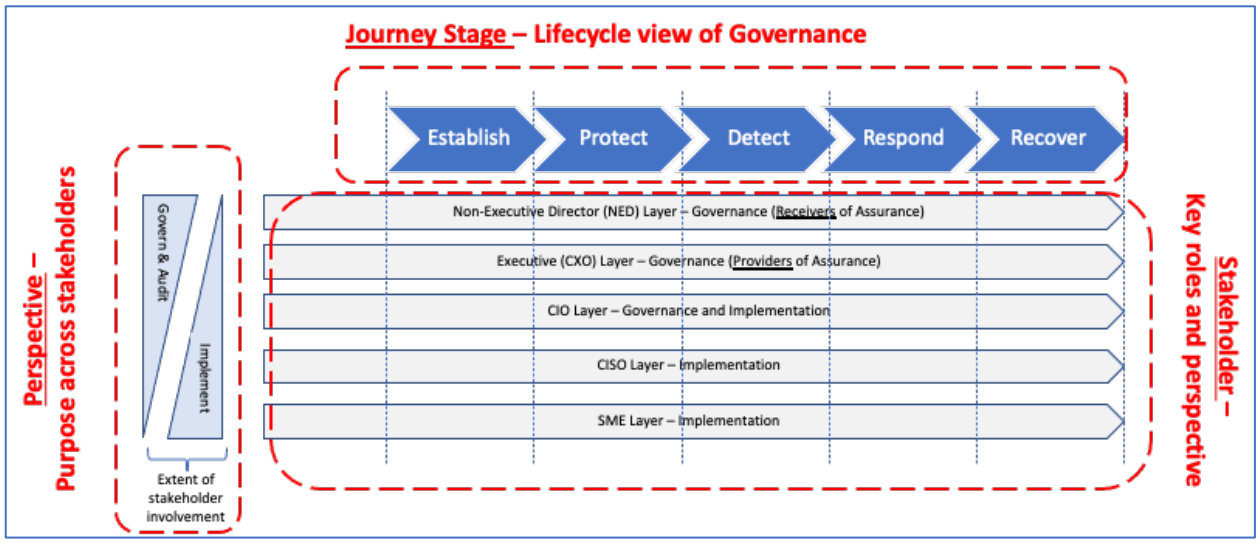

Figure 26: BCGF concepts

These concepts inform a more detailed view of components for helping NEDs and CXOs in cybersecurity governance as contextualised in Figure 27.

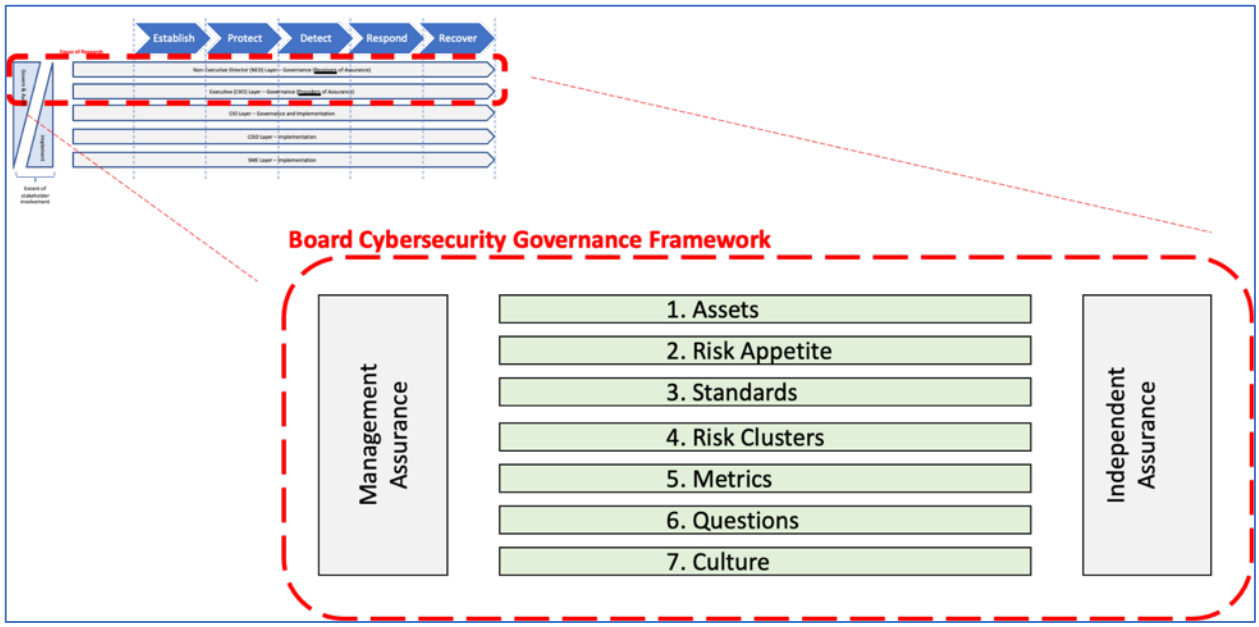

Figure 27: Context Diagram of BCGF

5.4 BCGF – Level 1 (Board View)

The highest level of the BCGF comprises a number of components. The term 'component' is generically used to describe elements in the BCGF. A component may be a process, a stage in the cybersecurity lifecycle, or a specific model in the framework. The BCGF offers a related set of components based on the research scope in hand. However, as research is an on-going process, additional views, concepts, or elements can be discovered and included as required over time to refresh the framework in context of further research and cybersecurity developments. The highest level (Level 1) of the model is a view to which NEDs can relate and enables the alignment of other implementation activities undertaken by CXOs and management. Level 1 is depicted in Figure 28.

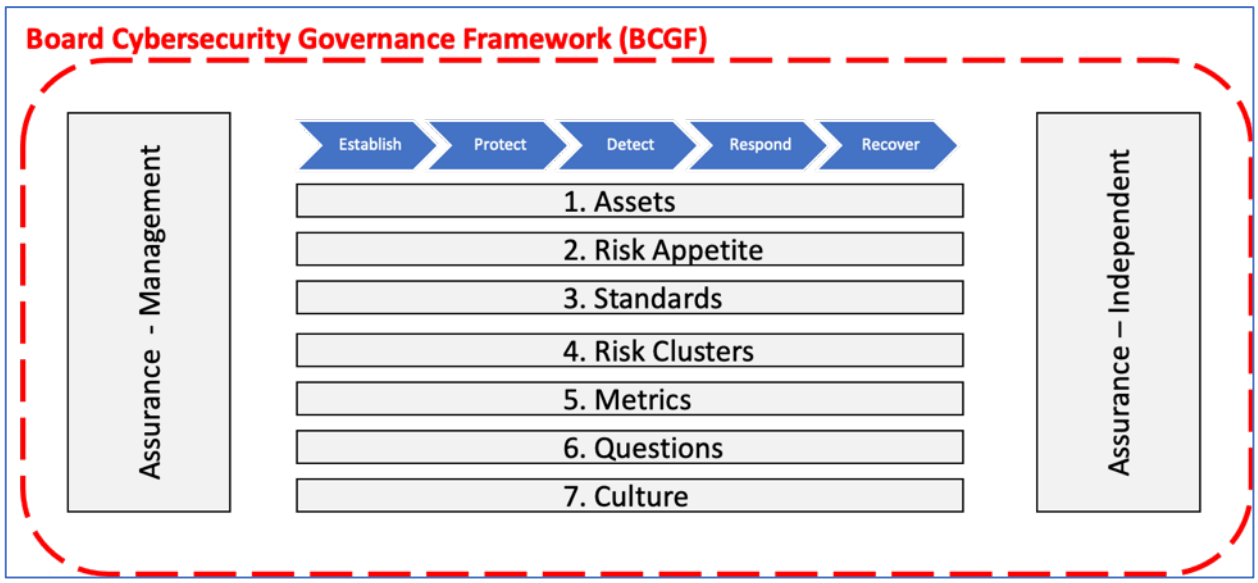

Figure 28: BCGF level 1 (board view)

Assurance bookends the BCGF in two aspects. First, this takes the form of assurance provided by management and second at the other end, assurance provided by independent sources. Assurance is a core part of governance, and in cybersecurity, this is a vital pillar due to the inherent complexity of the topic which demands the need for more specialist skills and know-how which often is not available amongst NED and CXO levels themselves. In addition to this, the 7 foundational models are represented under the cybersecurity lifecycle. Not all models may be relevant in an organisation due to its maturity,

focus areas or industry sector. The BCGF enables optionality by ensuring these models are standalone and can be used in isolation with others to ensure a fit-for-purpose and practical application. This flexibility is a vital aspect gleaned from the participant interviews and the expert evaluation workshop. For example, in many government organisations, the cybersecurity standards to comply with are very well understood and defined; not much choice in selection is necessary. Similarly, in private sector organisations that are regulated (e.g. banking, insurance, payments), mandatory compliance to specific minimum standards is required. The BCGF in such examples guides the extent to which standards over and above these should be pursued to attain greater levels of trust and competitive differentiation; this becomes a cost/value trade-off. The aims for each component in Level 1 of the BCGF are outlined in Table 31.

Component	Component Type	Aim of Component
Assurance – Management	Process	Assertion provided by executives to a Board on the extent of compliance to specific standards or targets. Often this can include audits, reviews and attestations from management.
Assurance – Independent	Process	Assertion provided by independent organisations or individuals on the extent of compliance to specific standards or targets. This can include external auditors, or subject matter experts (SMEs) qualified in cybersecurity reviews.
Cybersecurity Lifecyle	Process	The stages in cybersecurity governance that enable oversight of strategic and operational aspects. The aims and activities are detailed in the context of the needs of the NED and CXO stakeholders.
Establish Stage	Lifecycle Stage	Establish the critical assets to protect and agree on the risk appetite statement, along with the standards and thresholds for assurance reporting. This also includes setting the tone on the cybersecurity culture across the organization.
Protect Stage	Lifecycle Stage	Set the desired level of assurance (management v independent; desktop review v hands-on inspection) required on protection controls in place in the context of the threats and risk appetite.
Detect Stage	Lifecycle Stage	Set expectations on reporting and communications of events and impacts and receive notifications as appropriate with specific actions on their severity and importance.
Respond Stage	Lifecycle Stage	Endorse desired incident response actions required to internal and external stakeholders based on materiality and establish processes into the Board on notifications and approvals.
Recover Stage	Lifecycle Stage	Oversee processes for recovery from cybersecurity incidents. This includes understanding and improving the cybersecurity lifecycle from learnings in the response.
1. Assets	Model	Identify the business services and assets that warrant protection from cybersecurity risks. These include enabling processes, systems, data and vendors that enable consumer services.
2. Risk Appetite	Model	Outline the acceptable impact to assets from cybersecurity incidents. This includes share price and revenue impact, through to data loss, unavailability of services, and reputation damage.
3. Standards	Model	Agree on the standards that cybersecurity is to be governed against during implementation. These can be the baseline list and aspirational ones in the context of the industry sector.
4. Risk Clusters	Model	Identify a list of cybersecurity risk areas from environmental factors, to enable a targeted focus to risk management and education of the Board that is relevant and timely.
5. Metrics	Model	Establish and review metrics to ensure a wholistic approach to assurance and visibility of the implementation of cybersecurity across the security lifecycle.
6. Questions	Model	Assist in framing questions on cybersecurity so that greater clarity is provided in the scope and coverage of assurance and its

Component	Component Type	Aim of Component
		completeness in the context of the standards being governed against.
7. Culture	Model	Establishing a baseline of what the cybersecurity culture is through setting the tone to the audience and implementing indicators that inform its progress towards the desired levels.

Table 31: BCGF level 1 (board view) component descriptions

5.5 BCGF – Assets Model

5.5.1 Purpose

The Assets Model is used to identify and agree on the specific area(s) of the organization that warrant stronger levels of cybersecurity than others. This allows a risk-based approach to cybersecurity.

5.5.2 Business Scenario

The model is applied during business continuity and operational resilience discussions that examine the availability of services for customers and identify which ones should be protected as a priority. In addition, when making investment decisions, there is an imperative to ensure the most important areas of the organization's services receive appropriate levels of funding to manage risk.

5.5.3 Stakeholders

Stakeholders involved in the use of the model include NEDs who ultimately receive the output for review and endorsement. Other roles such as CXO, CRO, CIO/CISO and various risk / continuity experts will also use the model to draw up initial views for Board-level approvals. The model also enables informed discussions with relevant regulators of the organization in terms of the identification of critical assets.

5.5.4 Overview

The scope of business assets that require protection from cybersecurity threats can be broad for an organization. This can include the business services, processes, systems, and data provided to its stakeholders. It can also include specific people or teams in an organization and the protection of these (including their identity and special authorization limits) commensurate with their role in service delivery. Stakeholders can be customers, other businesses, or in the case of government organizations, the public at large. The broad breadth of business assets to protect can lead to a large cost base for cybersecurity risk management. An approach that classifies assets in terms of importance can be more economic and fit-for-purpose. The existing literature (Frank et al., 2019; Leech & Hanlon, 2017; Walton et al., 2021), participant interviews, and the expert evaluation workshop indicate the importance of a risk-based approach to cybersecurity to target investment in the areas that matter most. This includes ascertaining the higher priority areas (termed in industry and business as the crown-jewels) of an organization that warrant greater protection due to the criticality or importance to the organization. The Assets model enables a discussion to ascertain which assets are more important than others, based on the strategic and operational imperatives of the organization. This then leads to a risk-based approach to cybersecurity that is more practical. The Assets model is illustrated in Figure 29 and depicts a hierarchy of 6-dimensions that can be used to discuss and then agree which assets warrant specific protection from cybersecurity risks.

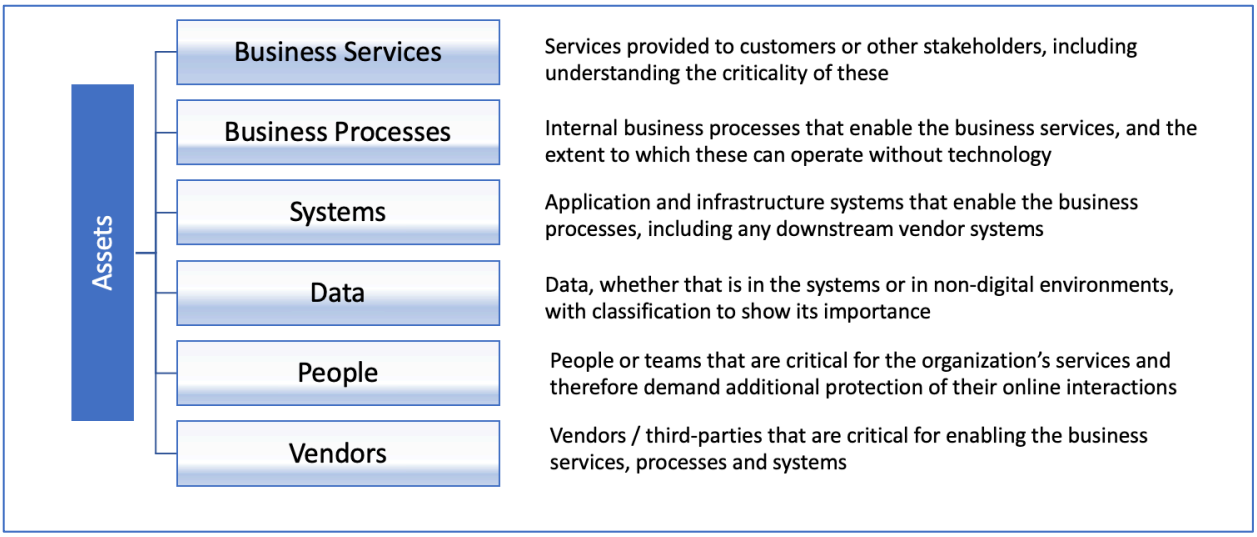

Figure 29: Assets model

5.5.5 Inputs

Business Continuity Plans (BCP) and related artefacts such as the Business Impact Analysis (BIA) are rich sources of information to highlight the importance of specific services provided by an organization (Torabi et al., 2014). This approach yields key processes that are important for continuity and highlight underpinning systems and data that need to be available in the event of an incident that impacts the confidentiality, integrity, or availability of a business service. In addition, the BIA often specifies the order of recovery for stakeholders should operational resilience be impacted. If the BCP and BIA are not available, then the 6 dimensions depicted in Figure 29 are a useful frame to discuss and agree on the business services, along with the underpinning processes, systems, data, people, and down-stream vendors that are of importance. This hierarchical relationship then is a core input into the model, and its identification and understanding should be pre-work ahead of any workshop to discuss and agree on the crown-jewels for cybersecurity resilience.

5.5.6 Implementation Guidelines

In a workshop style setting, business and risk subject matter experts who have knowledge of the BCP and BIA artefacts should be gathered. The first step is to identify and agree on a list of services and products provided by the organization. These are then analysed and placed in an order of importance that may represent higher, medium, and lower priority services. Factors to consider in this prioritisation in this discussion include:

- Impact to customer service if a process/system is not available for an extended period to relevant stakeholders (with specific discussion on the acceptable time period);
- Impact on revenue and reputation if the confidentiality, availability or integrity of the processes and systems is impacted; and
- Services that would result in a material impact to the financial viability of the company and cause concern to shareholders or regulators.

5.5.7 Outputs

The core outputs from the Assets model include the identification of business services into high, medium, or lower priority, as shown Figure 30. This could also be in the form of a tiering of business services, where Tier 1 is critical, and Tier 3 is of less importance. Organizations are free to use the classification that best aligns to their BCP and BIA equivalents. This classification then can be used to inform and identify the crown-jewels that warrant the most governance and protection in cybersecurity. Often these tend to be customer/consumer facing services, systems and data that would cause the most financial and reputation impact if these are unavailable or compromised.

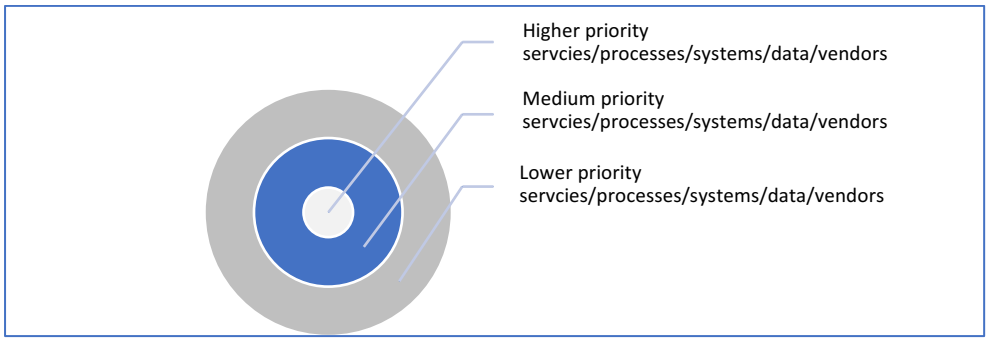

Figure 30: Asset model outputs

5.6 BCGF – Risk Appetite Statement Model

5.6.1 Purpose

This model is used to agree on the acceptable impact and acceptable consequences from a cybersecurity incident to the organization.

5.6.2 Business Scenario

It will typically be used in the situation or scenario where risk strategy is being discussed by CXOs and NEDs to explain the extent to which a cybersecurity incident is tolerable to an organization. Thresholds may be defined through the application of the model that then triggers the relevant incident response from the Senior Executives or the Board.

5.6.3 Stakeholders

The initial use is by relevant CXOs, CRO and risk SMEs to formulate an initial view of the risk appetite statement, as related to cybersecurity risk. Thereafter, the NEDs are presented with the output for discussion and review. The model also enables engagement with regulators of the organization in terms of the adopted cybersecurity risk appetite and how this is embedded in the risk management framework.

5.6.4 Overview

Whilst an organization may assume it will not be exploited or compromised in any form, in reality, this is more of a factor of 'when' it will be impacted by a cybersecurity event than 'if' it will be impacted. This impact can be widespread and affect the viability of an organization through a violation of the confidentiality, integrity and availability of the data systems (Corallo et al., 2020). As such, the model enables a realistic discussion and agreement of the impact that is not desired, and therefore can inform the commensurate level of controls to attain this. The cost of these controls is an inherent dimension, and this model brings in the economics of cybersecurity protection. If an organization wants minimal impact from a cybersecurity incident, then it naturally will need to invest more than one that is willing to consider some impact. Benchmarks from consulting companies or research houses like Gartner may inform such discussions, however the important factor here is that the level of risk the organization is willing to take impacts the required investment levels. The acceptable impact is analysed through the application of a series of business dimensions to agree on relative thresholds that will trigger concern for the NEDs and put the organization into an undesired state. The model allows other dimensions to be added or the stated ones to be removed. This level of tailoring offers a way to make the model fit-for purpose and evolve over time. The model informs CXOs and broader management teams to establish appropriate protection mechanisms commensurate with the parameters established through this process. This model considers impacts (from a cybersecurity event) to a range of dimensions such as

share price, revenue impact, data loss (acceptable numbers of data loss of customer/other data), operational resilience (acceptable downtime from cybersecurity event including recovery time objective), and reputational impacts (as measured by independent market organizations). Figure 31 outlines the related concepts in more detail. The generic scale associated with the dimensions ranges from 1-5 and enables absolute values to be tailored to each dimension for an organization. For example, 1 against 'customer data loss', could denote the loss of 1000 records of customer data, 2 could denote 2000, and so on. If a lower threshold is desired, then this could be 100, 200 etc.

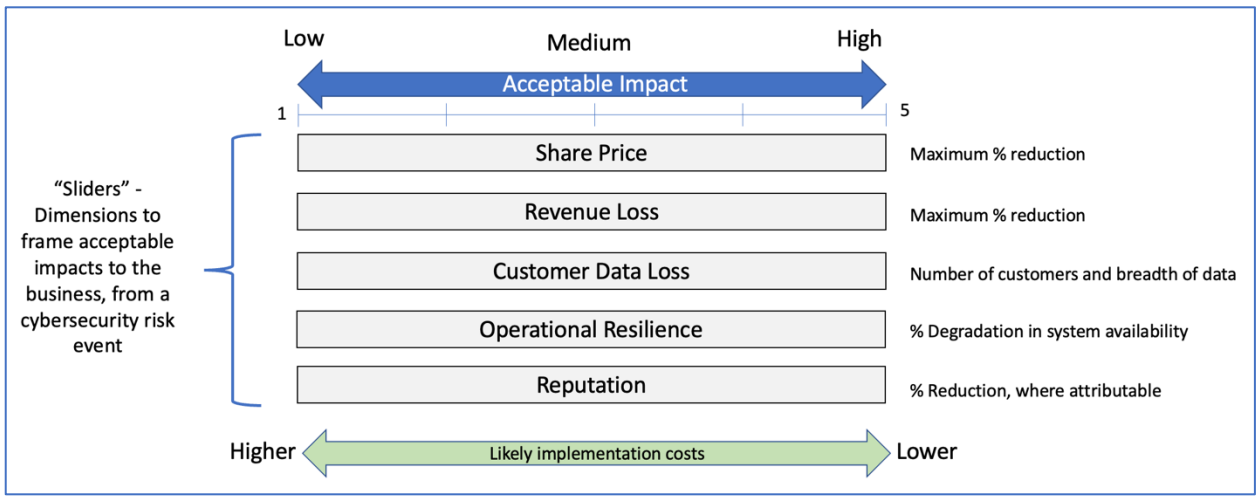

Figure 31: Risk appetite statement model

5.6.5 Inputs

Prior to a discussion with NEDs and CXOs, some pre-work to suggest the scale associated with each dimension in the model is required. The size and nature of the organisation and the risks it is willing to take will determine the absolute thresholds for each dimension and the scale to apply to the 1 to 5 scores. Typically, the risk community, led by the Chief Risk Officer (CRO) facilitates the initial scales to be used. This pre-work is in context of the organization's Risk Management Framework (RMF) which informs the inherent risks, likelihood, and consequences of risks. These are be refined and adjusted as necessary to support the cybersecurity governance needs of NEDs and other CXOs.

5.6.6 Implementation Guidelines

A discussion with NEDs results in an indicative view of where the acceptable risk for each dimension should be centred. This may not be one of the absolute values, but in fact, a desired range between 1 to 5. The score of each dimension can then be represented as one number or a range, and then can be an indicator of the risk appetite for the dimension. Aggregating these scores across all dimensions then gives an overall risk appetite, where an organization that has less tolerance for cybersecurity risk has a lower number than an organization that has no tolerance for cybersecurity risk. This spectrum of risk can then be used by management subsequently to prepare an outline of the expected implementation costs to attain the risk appetite. Costs should also include the impacts of an incident and the investment this may trigger for recovery. This trade-off in upfront costs and recovery costs (in the event of an incident) can enable insightful and informative risk discussions, and explicit agreement of the desired position. This exercise could be performed at the outset through engagement with the Board Risk Committee or the Chief Risk Officer, or as a second step following the risk appetite discussion.

5.6.7 Outputs

The outputs from this model are stated acceptable risk impacts for each of the dimensions and an aggregated score of these all together. The scale of 1 to 5 for each dimension and the ability to define the granularity of each risk level allows the model to be adaptable and extensible.

5.7 BCGF – Standards Model

5.7.1 Purpose

The standards model is used to understand and agree on the cybersecurity standards an organization should be adopting and against which its maturity and compliance program is based. It informs the nature of quality assurance to the chosen standard(s).

5.7.2 Business Scenario

The model is typically used when the risk strategy is being developed or refreshed to help guide and position such discussions in an informed manner against the model

5.7.3 Stakeholders

The initial use is by relevant CXOs, CRO and risk SMEs to formulate an initial view of the standard(s) that should be part of the baseline. Thereafter, the NEDs are presented with this for discussion and agreement and then receive assurance on compliance to the standard from CXOs ongoing.

5.7.4 Overview

This model enables NEDs and CXOs to understand and classify cybersecurity standards to identify which ones they should adopt for their organization. This is often fairly straightforward when it comes to mandatory standards in a regulated environment such as the energy and financial services sectors respectively in Australia (AEMO, 2023; APRA, 2019). However, research through interviews and the literature has shown the range of standards beyond the minimum regulated set to be large and often these are clustered in technical domains that do not provide clarity of the merits of one standard against the other. The danger in this is not having the right standard for the right point of maturity of the organization, which can create an incorrect cybersecurity posture that represents only the scope of the chosen standard. For example, some organizations may focus on a technical standard and not also have a standard that is focussed on process, people, or cultural aspects of cybersecurity. Adopting the right standards against which to access maturity is a critical step in cybersecurity governance as this represents the baseline against which to measure compliance against. This framework allows the positioning and discussion of the appropriateness of standards and then aids more informed selection as part of the assurance process. The standards model, as shown in Figure 32, can be used to classify the various standards available into those that are a minimum set, desirable standards and those that can act as a differentiator for the organization. Further, the model enables standards to be plotted against four dimensions that range from non-technical to technical and targeted at specific assets/parts of the organisation, or generic in nature. This model allows the positioning of standards and a better understanding of the coverage of standards in an organization. It is expected that the chosen standards will evolve as maturity is attained in one part of the model to other areas. For example, a financial services organisation may apply the PCI standard (targeted and deep technical) to the assets that process payments. Following compliance with this standard, it may evolve to a more generic scope across the organization to reduce broader risk.

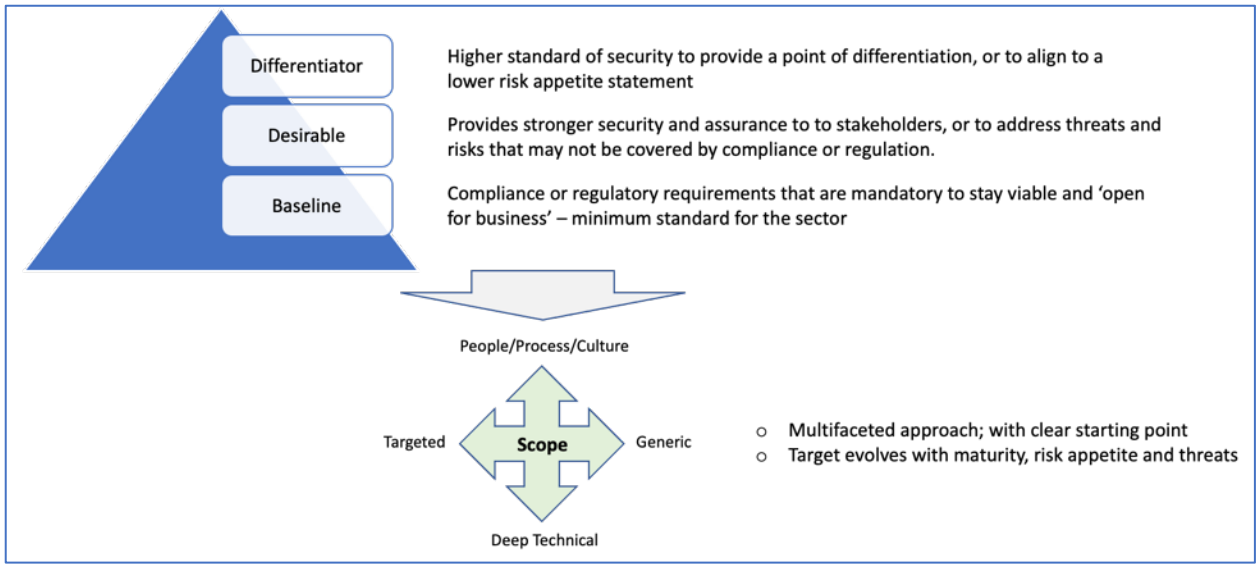

Figure 32: Standards model

5.7.5 Inputs

List of candidate standards for the industry and relevant for the organization are inputs, along with an indication of the minimum set for regulatory purposes. This list can be derived by Chief Risk Officers, General Counsel, or Auditors.

5.7.6 Implementation Guidelines

This model is initially used by risk or legal professionals to identify the full list of candidate standards and then classify them into the various dimensions. This is then followed by a recommendation, discussion, and agreement with NEDs on the sequence of compliance effort. This exercise is best performed after the risk appetite statement has been agreed on as that then informs the level of cybersecurity that is desired and the level of risk the organization is willing to take. Of note is that ongoing reporting and assurance then should be against the extent of compliance to this standard and noting any exceptions.

5.7.7 Outputs

A stated set of standards for compliance now and then in the near future. This can often be expressed as a 3-4-year roadmap depending on the maturity, size, and complexity of the organization. It is vital that the minimum baseline in the model is understood and agreed on for the organization and the sector in which it operates. This enables a focus on the more important and foundational standard at the outset. For example, a financial services entity regulated by APRA would have CPS234 in its baseline (APRA, 2019). Assurance activities (by management and independent reviews) can then be in the context of these chosen standards and as maturity is attained in a specific standard, the effort can move towards another for a continuous approach in the context of an increasing volume and sophistication of threats (Pienta et al., 2020). By way of example, for a regulated financial services entity that processes financial payments, the 'baseline' standards that are regulated by APRA are CPS234 Information Security (APRA, 2019) and CPS510 Outsourcing (APRA, 2010). Further, if the organisation processes payments, then compliance to the Payments Council Industry standard, PCI (2018b) is also mandatory. Standards that are 'desirable' and 'differentiator' as per Figure 32, could be international standards such as (ISO, 2013a, 2013b, 2018).

5.8 BCGF – Risk Clusters Model

5.8.1 Purpose

This model enables NEDs and CXOs to identify cybersecurity topics that articulate the key risk areas for the organization, or those that may be relevant from a broader industry perspective in the near future. This enables a more targeted approach to education, awareness, and risk management. The resultant risk clusters then augment regular compliance programs in place against specific standards chosen by the organization.

5.8.2 Business Scenario

The model is typically used in annual risk planning meetings or workshops as a way to inform focus areas and potentially have input into audit plans. The horizon of the risks identified can be 0-3 years and this then determines the sequence and importance of relevant items.

5.8.3 Stakeholders

NEDs use this model to form a view of their own top risks based on internal and external data points. CXO roles, including CEO, CFO, CRO and CIO/CISO, formulate a viewpoint and use this in discussions with the Board of Directors.

5.8.4 Overview

The Risk Clusters model, as shown in Figure 33, can be used for a range of areas including focusing management attention on these topics, formulating director education, regular cybersecurity assessments, and formulation of rolling audit plans to provide assurance to the Board. The field of cybersecurity can be broad and the network of systems and threats is ever changing (Zhao et al., 2019). The model enables the identification of topics that should be front of mind, based on internal posture and external factors in the immediate period. Internal themes are often informed by risk registers, penetration tests, and other audits that may identify areas for further improvement. These, however, do not bring in cybersecurity risks that are yet to materialise and are often related to new threat vectors outside of the organization. Therefore, external factors become really important and can inform any changes from regulators, incidents in the industry at large, and the trend of threats that are arising more broadly. Over time, knowledge of cybersecurity will improve due to the focus on just-in-time education that is informed by external and internal risks across short- and medium-term horizons.

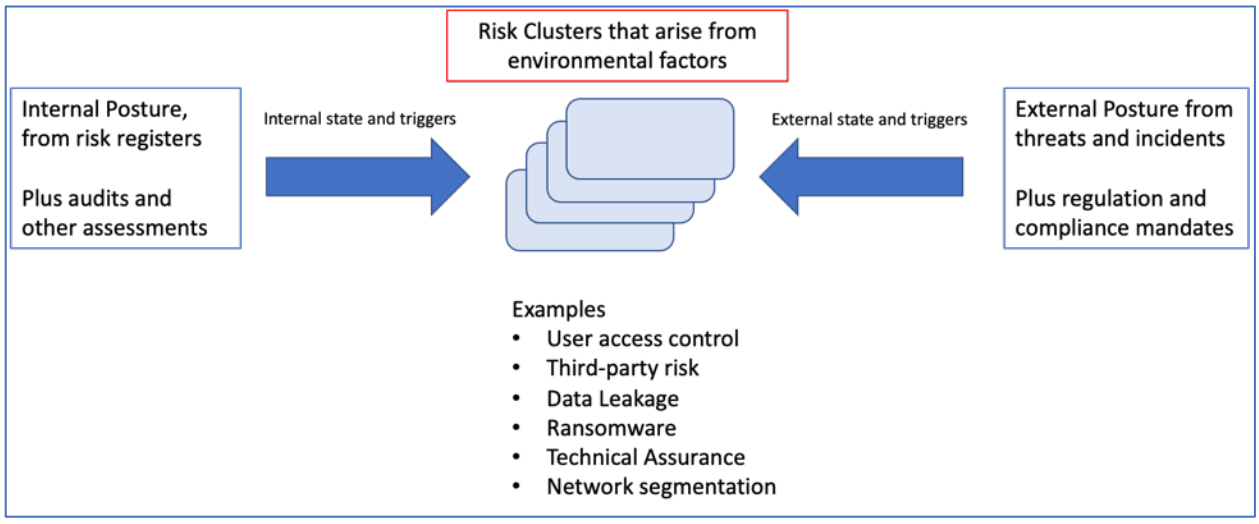

Figure 33: Risk clusters model

5.8.5 Inputs

There are two broad inputs, the first from internal source, and the second from external factors. The internal posture of an organization is often informed by risks that may be documented in risk registers or informed by management self-assessments and independent audits. These action registers can be a rigorous way to inform the themes that are relevant from an internal perspective, and therefore demand attention in the period ahead. The external posture is informed from changes and focus from relevant regulators who may be strengthening their focus based on industry themes, or intelligence only they may have. This posture may also be informed by cybersecurity threats and trends being observed through incidents.

5.8.6 Implementation Guidelines

Once the internal and external posture has been examined, the themes at an aggregate level can be synthesised from this. The aim here should be to identify a small number of themes, typically 7-10, that encompass the posture. Examples of themes include user access control processes, ransomware protection, and phishing defences. The exercise to identify risk clusters must be explicit and initially performed by relevant CXOs such as the CRO, CIO and COO. This then allows the output to be presented to NEDs for final agreement. These themes are refreshed on an annual basis as maturity is attained in these and also to factor in other themes that may have materialised since the last review. This approach also informs the education curriculum for the Board so that cybersecurity literacy can be planned in the context of these risk clusters to make it meaningful. Over time, knowledge of cybersecurity amongst Board Directors will improve due to the focus on just-in-time education that is informed by external and internal risks across different horizons.

5.8.7 Outputs

The core output is 7-10 risk cluster themes to guide the agenda and focus on the coming period. This allows a risk map or matrix to be established for these clusters, and a targeted focus to educate NEDs and business CXOs on the risks, impacts and actions to take for each risk group. Each risk cluster should be risk rated so that the relative risk of these can be depicted on a risk matrix to enable focus and visibility.

5.9 BCGF – Metrics Model

5.9.1 Purpose

The Metrics Model assists NEDs in validating the coverage of cybersecurity metrics they may receive or wish to receive. The volume and complexity of data can be large in cybersecurity and assurance through metrics can mask the underlying risk posture if they are not presented appropriately. This model enables NEDs to evaluate the scope and coverage of metrics to minimise the likelihood of blind spots in risk profile.

5.9.2 Business Scenario

Typically, this model is used when a new standard is chosen as the baseline for compliance or if the maturity of cybersecurity has changed (becomes better or worse) and refinement is necessary in the assurance reporting the Board receives.

5.9.3 Stakeholders

NEDs apply the model to give feedback to CXOs on areas they need to focus on for greater levels of visibility of the state of cybersecurity. CRO and CIO/CISO should formulate a recommendation of metrics and demonstrate the coverage through this model.

5.9.4 Overview

Appropriate metrics are an industry challenge which been described by Gartner as an area that has not been addressed by many organizations and that those that have, tend to only look at trailing metrics (Proctor, 2021b). Cybersecurity metrics for NED and CXO audiences can often drown the audience with technical detail, and often not portray an appropriate view of the cybersecurity maturity and posture. Metrics should be used to inform Board audiences on the highlights and lowlights of the cybersecurity defences and the areas where residual risk remains. The model is outlined in Figure 34 and defines the characteristics of good metrics as being actionable, comparable, and finally measurable in an accurate way. These are the critical dimensions of good metrics. An example of ineffective metrics is quoting the number of attacks a network perimeter faces each day. Whilst this can be interesting, it is of limited value as its not actionable or comparable to what a baseline should be. Use of the Metrics Model assists in validating that the organisation has the right metrics. Additionally, some metrics evolve as the maturity of the cybersecurity changes and the model enables an ongoing review of the appropriateness of these. The model classifies metrics that may be in a scorecard across four dimensions, leading/lagging and technical/business. This matrix enables an understanding of where there may be a concentration of too many metrics, or where there may be a gap in coverage that needs to be addressed. In addition, certain metrics are unique to the stage of the cybersecurity lifecycle presented earlier. So, using this matrix in the lifecycle enables discussion and agreement of metrics unique to each stage. For example, in the Establish stage, the number of exemptions granted from cybersecurity policy and standards would be useful lagging business metrics to ascertain the risk that has been accepted. Consciously looking at the spread of metrics across the lifecycle allows gaps to be discussed with more of a fact base. The model allows a more structured approach to metrics and as a result, NEDs will be more confident when governing cybersecurity and will be able to make stronger statements on the posture of cybersecurity risk and where they want more maturity and focus (Bailey et al., 2020; Mandy et al., 2021).

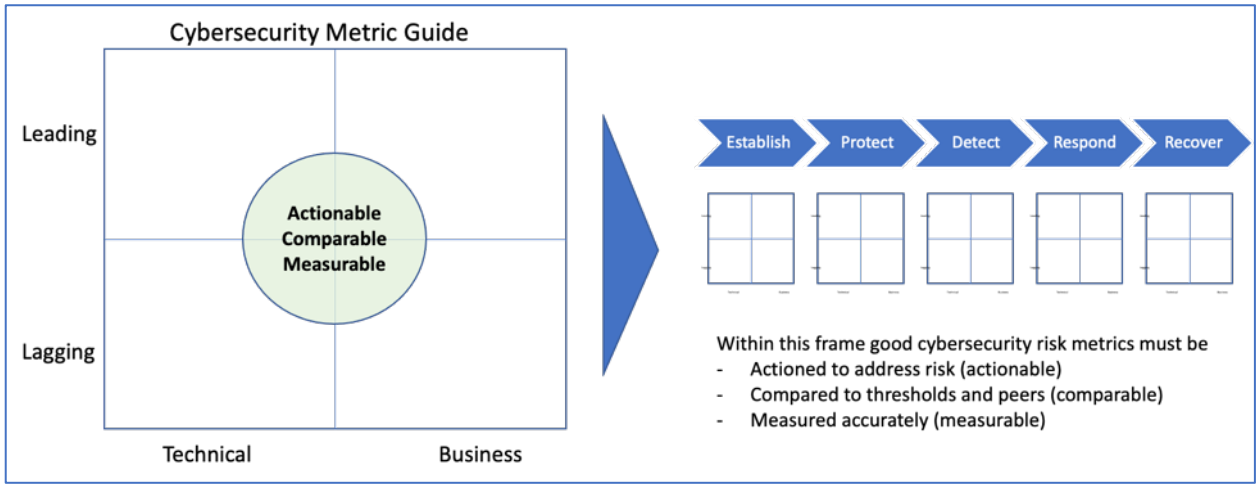

Figure 34: Metrics model

5.9.5 Inputs

The current set of metrics a Board is presented with are a key input into this model. These metrics are informed and guided by the cybersecurity standard that has been chosen to comply with. Each section or control requirement in the standard then shapes an appropriate metric to potentially include. For example, if a standard requires that operating systems are patched in 2 weeks, then the metric could be the number of servers that are not patched within this period. An additional detail could be the list of business services which are at risk as a result and whether these services are business-critical ones (as per Figure 29: Assets model, which highlights the important ones from a continuity perspective).

5.9.6 Implementation Guidelines

Typically, the CIO, CISO and CRO should formulate a list of metrics and map them into the Metrics Model as a starting point. These then need to be reviewed to evaluate the coverage against the cybersecurity standards adopted to ensure that the metrics do in fact cover key processes or controls that are required. The metrics should give assurance on core aspects of the standard. Following this, it could also be appropriate for the audit function to conduct a review, ahead of presenting the proposed metric scorecard to the Board.

5.9.7 Outputs

The output is a classification of cybersecurity metrics into the Metrics Model to show the concentration of these in specific parts of the lifecycle and in each of these, the quality of the metrics themselves in terms of the extent to which they are actionable (for decision making), comparable for peer comparison where appropriate, and also measurable easily in a quantified manner. The aim is to identify 4-6 metrics per stage that are the foundational ones, spread across the 4-box metric guide. This way the overall metrics in a scorecard is 20-30. An extension of the model is to use the identified metrics to then derive an overall security rating or security index. This allows a single number to be assigned and tracked as an aggregate score of maturity, which has been discussed by Rantos et al. (2012) who argue that security awareness metrics can be aggregated into a single evaluation score that can then be representative of the underlying maturity. Such an approach is built into some industry security monitoring tools where thresholds determine the score that is assigned to depict maturity.

5.10 BCGF – Questions Model

5.10.1 Purpose

The Questions Model provides a basis upon which NEDs can probe and clarify cybersecurity posture in a fact-based manner with more certainty of covering the key areas of scope. Whilst NEDs are adept at such questioning in business aspects of an organization, cybersecurity presents unique technical and non-technical concepts and so framing questions in potentially unknown areas is critical for a NED.

5.10.2 Business Scenario

When cybersecurity papers are presented to the Board, the model can be useful to structure the questioning in a topic that is technical and complex. This can be during assurance or compliance reporting or in fact when new investments are being proposed.

5.10.3 Stakeholders

NEDs are the primary stakeholder group that would apply the model, however CXOs would also use this when engaging roles that are implementing cybersecurity risk controls.

5.10.4 Overview

Asking questions to clarify, understand and also set the tone from the Board is a core tenant of a NED's role. On cybersecurity matters, the approach to this has a significant bearing on understanding the risk and maturity of cybersecurity controls. A number of industry papers and literature identify key questions NEDs should consider (CAQ, 2018; CII, 2016; Olyaei & Wheatman, 2020; Proctor, 2021a; Safi et al., 2021). The literature provides specific sets of questions, which over time can become dated or irrelevant to the specific organization being governed by the NEDs. The literature does not provide generic constructs that can be used to formulate effective questions to understand the state of

cybersecurity. Figure 35 provides a set of dimensions that can be used to think through and determine the questions to ask in a Boardroom setting. This has benefit in understanding the immediate scope or topic at hand, however it also has the added benefit of assisting in director education as this approach is adopted in the formulation of questions. The model centres on understanding the coverage of the question being asked across three dimensions; the cybersecurity lifecycle; the breadth of the assets or stakeholders being discussed; and finally, the depth in the systems architecture to which the response should pertain. These three dimensions, when thought of explicitly, assist in formulating more informed and specific questions. Further, assurance is a key component of this model, and NEDs need to consider the extent to which they are placing reliance on management assurance or independent assurance for verification of the answers. An aspect of this is whether the assurance is a desktop review or physical inspection of controls, and if this involves inspection, the extent to which this involves some intelligence sampling of the controls or a full review. Further, this covers continual assurance, not just a point in time and it is important this is discussed, and the extent of this continuous assurance is agreed on explicitly when it comes to cybersecurity controls. These aspects of the Questions Model make it generic and more easily applicable to different situations, organizations, and industry sectors.

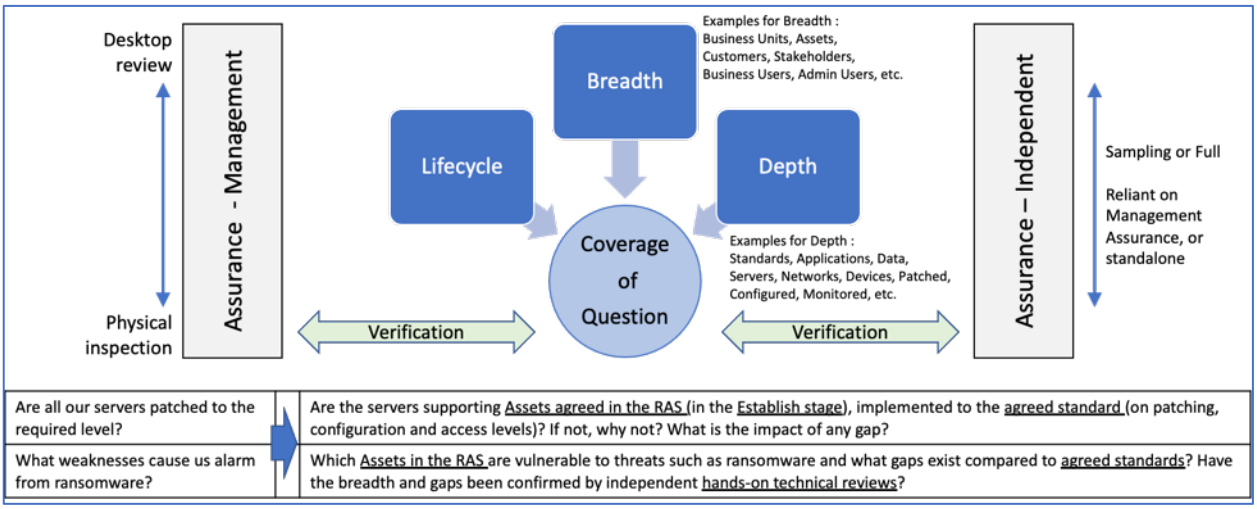

Figure 35: Questions model

5.10.5 Inputs

The input to this model is identification of the topics / areas that warrant probing when reading relevant Board papers or when setting the tone for risk management. These areas of questioning can then be guided and clarified by applying rigour as outlined by the dimensions in the 'coverage of question' in the Questions Model. An example could be a focus on the compliance of servers to the chosen standard. In this, the matter that is important is to better understand the extent to which servers are being maintained appropriately in accordance with selected cybersecurity standards.

5.10.6 Implementation Guidelines

In the example identified, the application of the Questions Model can generate a more precise and informed question to gain clarity on the state of the servers that support the most important business services and the extent to which there is compliance with the chosen standard. The question then evolves from a simple 'are all our servers patched to the required level' to 'are our servers that support the high priority assets in the RAS implemented to the agreed standard?'. This then leads to follow on questions of 'If not, then why not and what is the impact of the gap? When will they comply and who will independently assure the physical implementation?'. Hence, the model results in a number of clarifying questions that tease out the true state of the cybersecurity posture.

5.10.7 Outputs

The specific outputs from the Questions Model include the better clarity and structure of the questions being asked, which then leads to more informed discussions and a better understanding of residual risks in the organization. This can then inform the extent to which the risk should be accepted or mitigated with appropriate investment. An additional aspect of using the model is to improve the knowledge of NEDs and Senior Executives through consideration of the coverage (across the 3 dimensions in the model) their questions may cover (or not cover). This, over time, can be used as an education piece.

5.11 BCGF – Culture Model

5.11.1 Purpose

The Culture Model enables NEDs to better set the tone for cybersecurity across an organization and also enable its measurement across key areas.

5.11.2 Business Scenario

The model would typically be used in risk strategy discussions covering the desired and current risk culture across an organization.

5.11.3 Stakeholders

NEDs are the primary stakeholder group for this, though CXOs should also gain value and use from this as they drive out broader cultural change in the organization.

5.11.4 Overview

Culture across an organization can articulate the values and behaviours and through this, creates a positive ecosystem for cybersecurity (Brown et al., 2017; Rantos et al., 2012). Some argue that a culture that is aware of the need for good cybersecurity and the inherent risks the organization faces is one that can help reduce errors and complacency in operational processes (Donalds & Osei-Bryson, 2020; Winnefeld Jr et al., 2015). It should be noted that cybersecurity culture is a subset of the overall culture of an organization and is therefore dependent on broader values and ethical processes and behaviours. As such, guidance for NEDs and CXOs in the context of cybersecurity culture is extremely important. For NEDs, the aim is to set the right tone and expectations for cybersecurity and to also periodically determine the extent to which the culture is aligned to the desired state. A number of indicators can give insights on culture and this model assists in setting expectations across some key dimensions, as well as assist in establishing foundational measurements of progress over time. The measurements of culture need to be in the context of the relevant organization and so the initial set upon which to build or adapt is outlined. Key is that the indicators cover the cybersecurity policy compliance, behaviour of people, and also physical aspects such as safeguarding data.

Figure 36 illustrates the elements of the model. These are set on two aspects, how to plan for setting the cultural tone, and second how to measure and monitor the effectiveness of this.

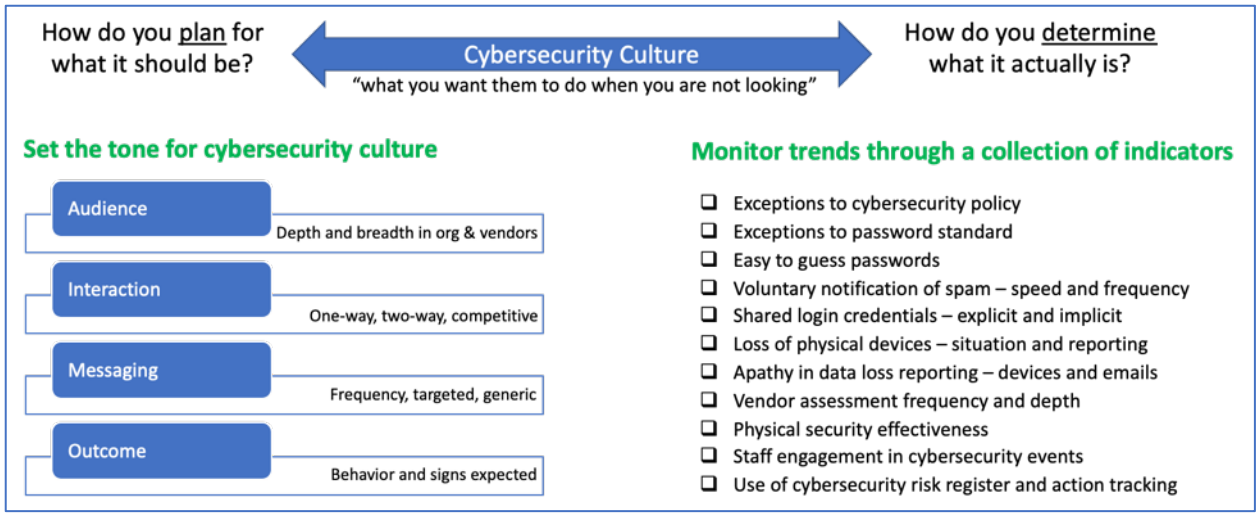

Figure 36: Culture model

When planning to set the tone on culture, the model provides four elements for NEDs and CXOs to consider, as detailed in Table 32.

Element#	Cultural Element	Description
1	Audience	The stakeholders they specifically target in terms of sections of the organization, vendors that support the organization and with consideration of the depth to which the messaging should be targeted.
2	Interaction	The style of engagement they expect from CXOs (or themselves in some cases) with the audience, which can be one-way information dissemination, or a two-way dialogue at appropriate forums, such as company townhalls, or all-hands meetings.
3	Messaging	The nature of communication, in terms of if it is targeted on specific topics or audiences, and also being explicit on the frequency. This ensures there is not a 'set and forget' approach to culture and it is taken as an ongoing effort to reinforce the tone.
4	Expectations	The outcome and behaviour desired is critical to state so there is no confusion on what 'good looks like'. This step again is a reinforcement of the tone, and if done by NEDs, it is done right from the top.

Table 32: Cultural elements

When monitoring the culture, the model provides a collection of measures. These need to be chosen in context of the maturity of the organization and what is possible. One core element of culture that has been covered in literature is the behaviour of individuals in responding to peer pressure and wanting to be better in a competitive sense. This is often called gamification and can be a driver of a self-driven culture that learns and grows through reflection and continuous improvement as measures are shared across sections or divisions of the organization (Baxter et al., 2016; Yang et al., 2017). This approach leans on human behaviour desiring to compete and improve (Silic & Lowry, 2020). Whilst a series of measures are presented in the Culture Model, these should be refined in the context of culture discussions for an organization. Making these fit-for-purpose is critical and often they can be complemented by CXOs sponsoring mock exercises, simulations, and appropriate recognition of achievements in cybersecurity culture. Such approaches increase the muscle memory of an organization which improves culture and ensures it is more aware of risks and responses.

5.11.5 Inputs

For the first stage of implementation, the desired cybersecurity culture should be set against the four dimensions of Audience, Interaction, Messaging and Outcome. This can be a facilitated NED discussion

with starting points and options presented by the CRO or the CXO team collectively. The other input here are some metrics that depict the trend in cybersecurity culture over time. These should then be debated in the context of the desired tone. Finally, an overall view of the culture of the organization in its various divisions is a useful backdrop against which to discuss and apply the model.

5.11.6 Implementation Guidelines

The implementation is via a discussion and review by the NEDs of what CXOs have suggested as the cultural tone and how to monitor this. NEDs must examine this thoroughly as it may not be what is required from their broader and longer-term perspective. Critical review and feedback are essential from the Board on this. The measures chosen to track the culture and signs of improvement should be the right mix covering hard-wiring (compliance to policy, standards, and processes) as well as soft-wiring (behaviours, symbols, and indicators). Often publishing indicators and the trend can be a key mechanism for gamification across divisions and organisation and encourage a self-driven improvement. However, the use of such techniques should be carefully considered in the context of the broader culture and industry sector. Examples of indicators are given in Table 33.

Indicator #	Culture Indicator Description
1	Number of exceptions to policy or standards, especially the stated password expiry
2	Number of easy to guess passwords used across divisions
3	Speed of reporting in loss of data (laptops or incorrectly sent emails)
4	Volume of staff engagement in cybersecurity forums
5	Frequency and nature of voluntary reporting of incidents and issues/risks

Table 33: Examples of cybersecurity culture indicators

Once the desired culture has been defined across the four aspects and the initial sample of measures, it is important for management to formulate a communications and engagement plan to interact with staff, suppliers and other stakeholders involved in the operations of the organization.

5.11.7 Outputs

The agreed view of the cybersecurity culture across the four aspects, sample indicators and direction to inform a comprehensive communications and engagement plan are core outputs from this model.

5.12 Economic, Social and Governance (ESG) Relevance

ESG regulation is evolving across jurisdictions globally and is also a complex domain with a scope that is still being refined and agreed by regulators (Longo, 2023). As such, this research does not claim to provide a detailed investigation into this area. However, given this is a topic for Board Directors in their governance responsibilities, it is important to place it in context. The use of the BCGF aligns to the aims of ESG, as shown in Table 34. This is an important factor in the work of NEDs and CXOs. As regulations and frameworks evolve in this field, future research could investigate the feasibility of quantifying the value generated (in context of ESG parameters) through the application of the BCGF to cybersecurity investments in technology and people.

ESG Domain	Outcome/Impact from application of the BCGF
Economic	A more balanced risk-based approach to cybersecurity governance, that can lead to being more cost-effective. The assets that matter the most are then offered the most attention in safeguarding their confidentiality, integrity and availability.
Social	The footprint of protection is fit-for-purpose and from a people perspective, effort and resources can be applied more intelligently, with an indirect benefit to staff in the company being informed on the important priority areas to help in staff engagement.
Governance	Simplification of governance arrangements such that these are targeted and commensurate with the value and importance of the assets being protected. As maturity is attained progressed to lower priority areas is then possible.

Table 34: ESG relevance of BCGF

5.13 Implementation of BCGF overall

Prior sections discussed each of the 7 foundational models individually, in terms of their purpose, scenarios for usage, inputs, implementation, and outputs. The BCGF has been designed so that each model stands alone to allow implementation that is fit-for-purpose for an organization and enables the framework to be applied in whole or part. The breadth of the application is determined by the current maturity of the Board in regard to cybersecurity governance. From a holistic perspective, it is important that the BCGF is not seen as a separate set of artefacts for Board governance that resides outside Board processes and relevant sub-committees. Embedding cybersecurity risk discussions into the Board governance processes such as strategy, assurance, risk and business performance is critical so that it is seen as an enabler of the business, and not something that sits outside of this. The Corporate Governance Framework, AICD (2024a) represents the director practices essential across quadrants representing the individual director, the Board, the organisation and other stakeholders. The applicability of the BCGF within this context is shown in Figure 37.

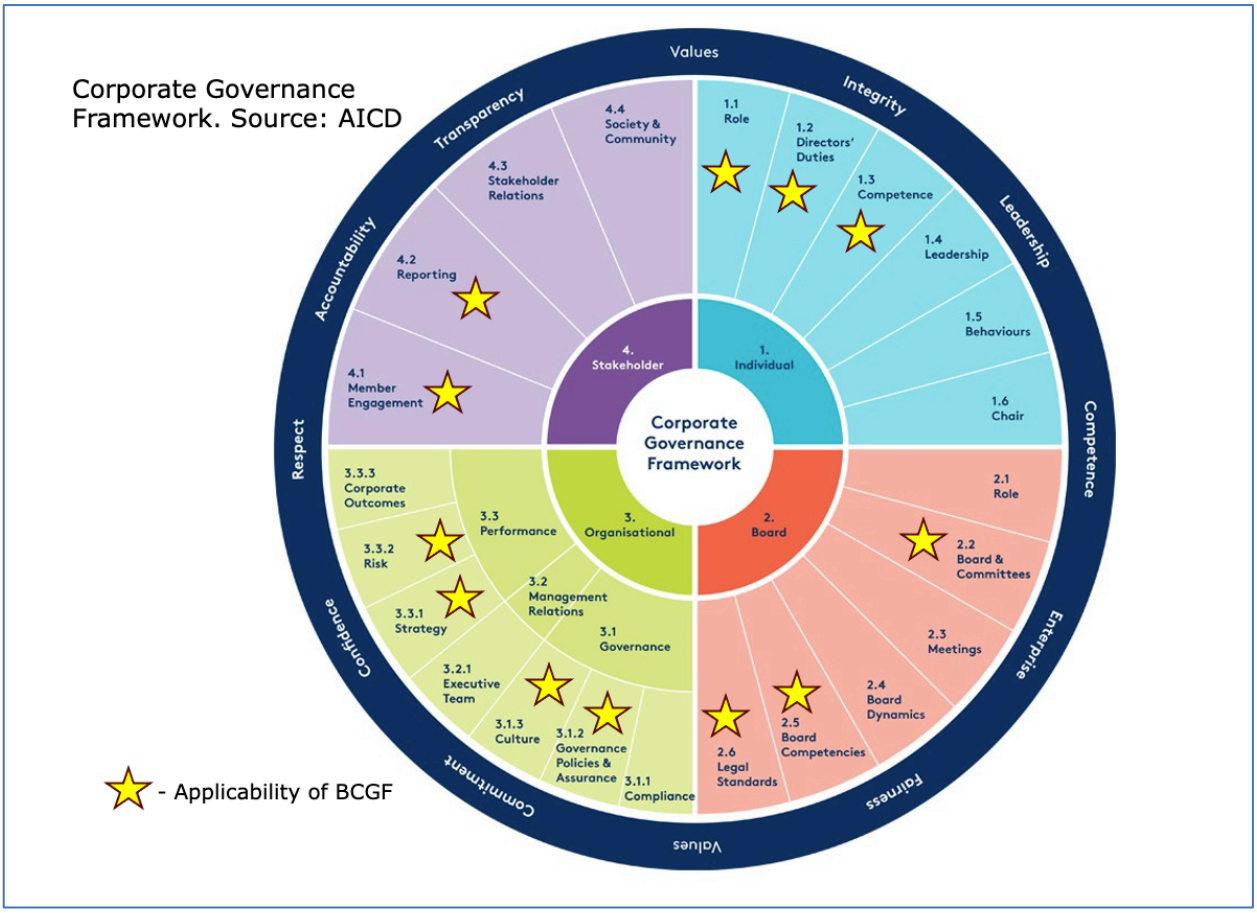

Figure 37: Applicability of BCGF in board governance (AICD)

5.14 Summary

This chapter detailed the BCGF that was developed and evaluated through this study. It covered the 7 models in the framework and the way they can be applied or instantiated in Board cybersecurity interactions in organizations. The BCGF as a whole and its 7 foundational models individually can address the RQ in terms of providing a framework to help non-technical audiences such as Board Directors and Senior Executives to enable them to better govern cybersecurity. The next chapter focuses on the framework evaluation, which includes data and insights from interviews, feedback from the expert evaluation workshop and expert evaluation survey. The results of the evaluation and learnings will also be discussed in the next chapter.

6 Results and Evaluation

6.1 Introduction

This previous chapter detailed the proposed BCGF, including the 7 foundational models within this, and how the framework can be applied or instantiated for Board-level cybersecurity governance in an organization. This chapter deals with the framework evaluation, which includes insights gleaned from the interviews, feedback from the expert evaluation workshop, and expert evaluation survey. In addition, correlation of the concerns raised in interviews to the models in the BCGF provides additional confirmation of the ability of the framework to address the RQ in terms of providing a framework to help Board Directors and Senior Executives to better govern cybersecurity. This systematic approach to evaluation is shown in Figure 38.

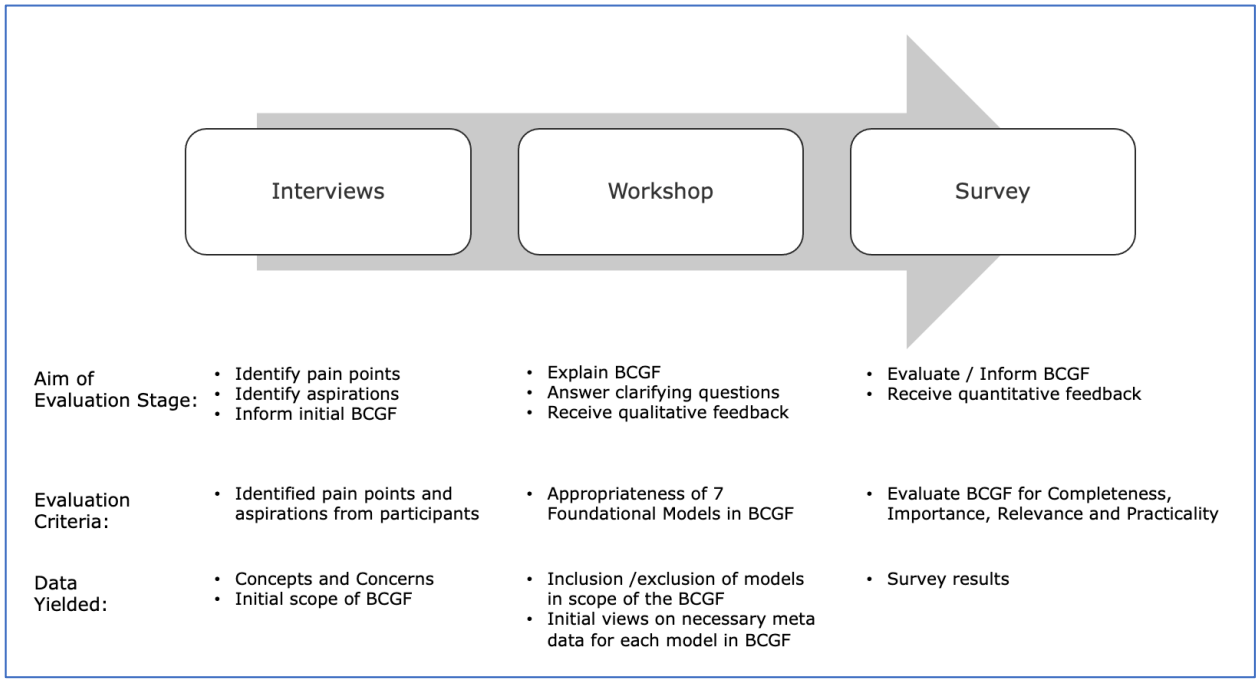

Figure 38: Evaluation stages

6.2 Data Gathering – Interviews

6.2.1 Participant Experience

Central to the research was to engage 15 highly experienced participants that have held or are holding roles as a NED, CIO, or CISO. Further to their expertise, their breadth of experience across multiple industry sectors was critical to ensure nuances across organizations and industries was harnessed. Five experts in each role were included in the one-on-one interviews. The extent of their experience was more critical and important than the number of participants interviewed due to the specialised nature of Board cybersecurity governance. The average industry experience for the interview participants was 34 years, and participants as a whole covered the key industry sector codes outlined in the International Standard Industrial Classification. The criteria used to identify participants is provided in Table 35. Details on the experience of the actual participants interviewed in terms of their professional experience and industry coverage is shown in Appendix 8.3 (Table 57 for professional experience and Table 58 for industry coverage).

Role	Criteria for participant selection
ALL	Extent of professional experience > 15years industry – based on public profile on LinkedIn, organizational websites, or company annual reports.

ALL	Experience across multiple industry sectors in multiple roles to ensure coverage across a broad breadth of businesses and their nuances.
NED	Held Board Director roles (or equivalent) that were accountable for the organization, including its cybersecurity posture.
CIO/CISO	Held Senior Executive roles that reported to Boards to provide assurance and reporting on cybersecurity matters.

Table 35: Criteria for identifying participants for interviews

6.2.2 Interview Questions

The aim of the participant interviews was two-fold, first to capture the pain points and aspirations NEDs, CIOs and CISOs had in Board cybersecurity governance, and second, the nature of the solutions they proposed to address these (where they had a perspective of these). This feedback assisted in informing the BCGF. Two sets of interview questions were used with participants, depending on whether they were a NED or CIO/CISO. This approach allowed discussion from two perspectives, those who had expertise in governing from a Board perspective (NED) and received reports and status on cybersecurity, and those who had experience in presenting to a Board on the cybersecurity posture (CIO/CISO). These perspectives enabled different viewpoints to be gleaned and then compared for alignment or divergence. In some cases, participants had held both categories of roles. In this case, their primary role was taken in interviews. The questions presented in the interviews are outlined in Appendix 8.5.2 (NED) and Appendix 8.5.1 (CIO/CISO).

6.2.3 Insights from Interviews

The interviews were conducted virtually in some cases, and others were in person to accommodate the preferences of participants. Prior to these interviews, participants were sent a series of questions to consider in regard to the pain points and aspirations they had from Board cybersecurity governance. These questions are detailed in Appendix 8.5 and were structured for participants that receive cybersecurity assurance (NEDs) and those that provide assurance (CIO and CISO). The discussions in each of the interviews were synthesised into a framework that coded and classified insights into categories, as shown in Table 36. This approach augmented the DSR method with GT techniques to drive out more detailed synthesis. This enabled the identification of concepts that were frequently raised by participants and therefore could be the focus point in the research. In addition, the participant pain points and aspirations were collectively synthesised to a series of 'concerns' they had articulated. This allowed another dimension for the evaluation of the final BCGF, in terms of correlating these concerns to the models in the BCGF that helped to address them.

Category	**Description**
Party	Person, role, group, or organization
Process	Manner in which a set of activities are conducted
Event	An outcome or trigger that results in an action
Object	A noun or other significant item that plays importance in a process or event
State	The status of an activity or party
Metrics	Artefacts that allow the measurement of the status or posture of an entity
Standards/Frameworks	Industry standards and frameworks for cybersecurity

Table 36: Categories of concepts in interviews

The resulting mapping of interview concepts into these categories is shown in Table 37. This mapping informed the 7 foundational models in the BCGF, including the guidelines on their implementation. The count represents the number of participants who mentioned the associated concept and the highlighted ones depict concepts mentioned by 5 or more participants.

PARTY			PROCESS			EVENT			OBJECT			STATE			METRICS			STANDARDS / FRAMEWORKS		
Name	Role (NED, CIO/CISO or ALL)	Count	Name	Role (NED, CIO/CISO or ALL)	Count	Name	Role (NED, CIO/CISO or ALL)	Count	Name	Role (NED, CIO/CISO or ALL)	Count	Name	Role (NED, CIO/CISO or ALL)	Count	Name	Role (NED, CIO/CISO or ALL)	Count	Name	Role (NED, CIO/CISO or ALL)	Count
Board	ALL	7	Educate/Train	ALL	12	Continuity in meetings	ALL	4	Assets / Apps / Data	ALL	14	Time Allocated	ALL	8	Fit-for-purpose	ALL	6	ACSC Essential 8	ALL	6
Director	ALL	6	Switch Context	ALL	9	Quarterly ARC Update	CIO/CISO	4	Risk Appetite Statement	NED	10	Process Lifecyle	ALL	7	%Progress / Trend	ALL	5	NIST	ALL	5
CISO	ALL	5	Inform	ALL	6	Breach	CIO/CISO	3	Terminology/Language	ALL	9	Competant/Skilled	CIO/CISO	5	Comparison (Peer)	ALL	4	ISO	ALL	4
Advisors	ALL	4	Compliance (Competitive)	CIO/CISO	5	Cyber Incident	CIO/CISO	3	Controls/Framework	ALL	8	Mature	CIO/CISO	4	Story	CIO/CISO	4	APRA CPS234	ALL	3
CEO	ALL	4	Explain (Consequences)	ALL	5	Risk Accepted	ALL	3	Risk Cluster	ALL	7	Independent	ALL	3	Trends / Arrows	CIO/CISO	4	CIS 20	CIO/CISO	2
Customer	ALL	4	Q&A Presentation	ALL	5	Audit	ALL	2	Cost/Budget	ALL	5	Urgent	CIO/CISO	3	Dashboard	ALL	3	ISM	ALL	2
3rd Party	ALL	3	Questioning	ALL	5	Industry Cyber Event	CIO/CISO	2	Risk Profile	ALL	5	Awareness	NED	2	Fake Phishing	ALL	3	AESCSF	CIO/CISO	1
Big 4 Audit Firm	ALL	3	Cross-pollinate skills	ALL	4	Penetration Test	ALL	2	Risk Scenarios	CIO/CISO	5	End of Life	CIO/CISO	2	Lagging	ALL	3	CMMI	CIO/CISO	1
CIO	ALL	3	Maturity Assessment	CIO/CISO	4	Warning (Level)	CIO/CISO	2	Analogy	ALL	4	Important	CIO/CISO	2	Leading	ALL	3	COBIT	CIO/CISO	1
Executives	ALL	3	Mock Exercise	ALL	4	Board Annual Update	CIO/CISO	1	Culture	NED	4	Unskilled	CIO/CISO	2	Pyramid Structure	CIO/CISO	3	Defence in Depth	NED	1
Media	CIO/CISO	3	Risk Assessment	ALL	4	Seek Approval	CIO/CISO	1	IT and OT Risks	ALL	4	Breached	CIO/CISO	1	Reporting Structure	CIO/CISO	3	PCI DSS	CIO/CISO	1
Shareholder	ALL	3	Simulation	ALL	4	Threat Notification	CIO/CISO	1	3rd Party Risks	ALL	3	Business Background	CIO/CISO	1	Small Scorecard	ALL	3	Privacy Law	CIO/CISO	1
Audit & Risk Committee	CIO/CISO	2	Mapping	CIO/CISO	3				Data Lifecycle	NED	3	Careless	CIO/CISO	1	Visualisation	CIO/CISO	3	PSPF	CIO/CISO	1
Company / Organisation	CIO/CISO	2	Remediation	CIO/CISO	3				Risks (+Emerging)	ALL	3	Current State	NED	1	Balance Scorecard	CIO/CISO	2	VPSPF	CIO/CISO	1
Exec Committee	ALL	2	Build Rapport	CIO/CISO	2				Risks (Industry)	CIO/CISO	3	Design Effectiveness	NED	1	Cost Impact	CIO/CISO	2			
Insurance Companies	NED	2	Engage	CISO	2				Shareprice	ALL	3	Disgruntled	CIO/CISO	1	Graph	CIO/CISO	2			
Regulator	CIO/CISO	2	IT Processes	ALL	2				Threat Landscape	CIO/CISO	3	Exposed	CIO/CISO	1	Hierarchy	CIO/CISO	2			
AICD	CIO/CISO	1	Look inward	ALL	2				Business Services	ALL	2	Flatfooted	CIO/CISO	1	Highlights/Lowlights	CIO/CISO	2			
Coach	CIO/CISO	1	Look outwartd	ALL	2				Cloud	ALL	2	Illogical	CIO/CISO	1	League Table	CIO/CISO	2			
Consultants	CIO/CISO	1	Benchmark	CIO/CISO	1				Global Perspective	ALL	2	Known Unknown	NED	1	Posture	CIO/CISO	2			
Partnership	CIO/CISO	1	Case study Review	NED	1				Glossary	CIO/CISO	2	Logical	CIO/CISO	1	Risk Impact	CIO/CISO	2			
People	CIO/CISO	1	Communications Strategy	NED	1				Projects / Initiatives	CIO/CISO	2	Negligent	CIO/CISO	1	Target	NED	2			
Staff	CIO/CISO	1	Downstream	CISO	1				Ransom	CIO/CISO	2	Observer	CISO	1	Urgency	NED	2			
Stakeholder	CIO/CISO	1	Incident Response	NED	1				Authorities	NED	1	Operating Effectiveness	NED	1	Vendor Scores	CIO/CISO	2			
Steering Committee	CIO/CISO	1	Make Decision	CIO/CISO	1				Critical Infrastructure	CIO/CISO	1	Target State (sector)	NED	1	Averages	NED	1			
Vendors	CIO/CISO	1	Recovery	NED	1				Elevator Pitch	CIO/CISO	1	Unknown	NED	1	Business Parameter	CIO/CISO	1			
			Sensitivity Analysis	NED	1				Emails	CIO/CISO	1	Unknown Unknown	NED	1	Consistent	NED	1			
			Social Interactions	CIO/CISO	1				Gaming Theory	CIO/CISO	1	Visible	CIO/CISO	1	Coverage	CIO/CISO	1			
			Spend Analysis	NED	1				Insurance Premium	NED	1				End to End	CIO/CISO	1			
			Upstream	CIO/CISO	1				Key Risk Indicators	CIO/CISO	1				Frequency	NED	1			
			Value Assessment	NED	1				Legislation	CIO/CISO	1				Heatmap	CIO/CISO	1			
									OHS Policy	CIO/CISO	1				Insights	NED	1			
									Policy	CIO/CISO	1				Patch Levels	CIO/CISO	1			
									Regulation	CIO/CISO	1				Qualitative	CIO/CISO	1			
									Revenue	CIO/CISO	1				Quantitative	CIO/CISO	1			
									Risk Tolerance	NED	1				Salient Points	CIO/CISO	1			
									Roadmap	CIO/CISO	1				Speed of Reporting	NED	1			
									Talent Strategy	CIO/CISO	1				Thresholds	NED	1			
									Toxic Assets	CIO/CISO	1				Timing of Reports	NED	1			
									Translation Layer	CIO/CISO	1				Weaknesses	CIO/CISO	1			
									Veto-rights	NED	1									
									Vulnerabilities	CIO/CISO	1									
									Weakest Link	NED	1									

Table 37: Concepts synthesised from interviews into categories

The most frequently mentioned concepts as shown in Table 37 (highlighted) are discussed in the following to highlight the nature of the feedback received from the interviewees under each *category*.

Party and Process Categories

An aspect discussed consistently across the *process* category was the need for NEDs to stay abreast of new developments in cybersecurity, including the need to educate and train themselves on a regular basis. The aspiration was to have a just-in-time perspective to learning around the topics that were relevant for the organization's context rather than having to learn all aspects of cybersecurity that may or may not be relevant. It was posited that the internal and external environment informs threats and risks that should be the topics in this curriculum through the identification of risk clusters or themes. Risk clusters represent emerging themes that could become a risk from a cybersecurity perspective and therefore education around them was deemed to be a just-in-time approach. This learning approach was expanded in some discussions to the ability to ask the right questions and set the right tone in a generic way. Without this just-in-time education, NEDs were struggling to understand the aspect of cybersecurity being presented to them (given its breadth), and therefore were challenged in knowing what questions to ask. Further, the fact that they only tended to spend 1-2 days every 2 months in a specific company meant they had to context-switch between various Boards, and also be in tune swiftly on complex topics such as cybersecurity. This theme was expressed as a pain point and aspiration in terms of an area that warranted a smart solution, over and above attending courses, as it had to be relevant for the risk environment being governed.

Object Category

The concepts in the *object* category captured the needs for NEDs to set a risk-appetite statement that identified the critical assets in a company, given economically it was not affordable (or practical from a user convenience perspective) to have the same level of security to protect all assets in an organisation. This included the need to examine risk scenarios and the effectiveness of controls in that context.

State Category

The concepts related to the *state* category were centred on having a lifecycle approach to cybersecurity that understood the role and skills Boards needed to develop, including an understanding of the scope and effort to dedicate in each stage of the lifecycle.

Metrics Category

The *metrics* category captured discussion on what is an industry challenge, in having the right cybersecurity metrics that were fit-for-purpose for the organization's maturity, and also could show a trend of improvement or degradation. This was seen as a challenging area given the inherent technical complexity of cybersecurity and not knowing if the coverage and depth of metrics was appropriate.

Standards/Framework Category

Finally, the *standards/frameworks* category provides discussions on the fact there are too many standards and frameworks to understand, including the difficulty in identification of which of these would be relevant for the organization. Essential 8 and NIST were seen as aspirational standards to attain compliance to over time.

The discussions captured insights that were often presented as an aspiration, pain point or need. These insights have been synthesised into 'concerns.' For the purpose of this research, a concern is defined as an 'issue or need that Board Directors have expressed in regard to them governing cybersecurity, which if addressed through more guidance would assist in them being more confident in governing cybersecurity risk at a Board level. The core concerns represented in the most frequently mentioned concepts in expert interviews are detailed in Table 38. These are classified into whether they were expressed as a pain point or aspiration, and also whether the view was from the perspective of a NED or CIO/CISO. The concerns are important from a validation perspective to ensure these are addressed in the final BCGF arising from this research.

Concern #	Expressed as a Pain Point or Aspiration	Perspective of	Description
C#1	Aspiration	NED	Timely education and training based on topics informed by internal and external risk scenarios or events.
C#2	Aspiration	NED	Techniques to question the state of cybersecurity in a generic way so that unknowns are identified and understood more easily.
C#3	Pain Point	NED	Understand the scope of the organisation's assets, that are of highest importance for protection and cyber resilience.
C#4	Pain Point	CIO/CISO	Boards being unable to define the risk appetite for cybersecurity incidents, and where it exists, it is vague and not informing.
C#5	Pain Point	NED	Risk/Cost analysis of cybersecurity posture not explained clearly in risk discussions.
C#6	Pain Point	CIO/CISO	Never enough time is allocated to review and discuss cybersecurity posture with the Board.
C#7	Aspiration	NED	Understanding cybersecurity in terms of the lifecycle would assist in focus and narrowing down discussions to specifics.
C#8	Pain Point	NED	Cybersecurity metrics are not meaningful, difficult to ascertain if they have the right breadth and depth; trends cannot be easily seen.
C#9	Pain Point	NED	Not clear on which standard is appropriate for compliance and the rationale for this is not presented in an independent manner.
C#10	Pain Point	NED	Executives rarely present a view of the criticality of various assets (systems, data, people, or process) to enable a cost/risk focus.
C#11	Pain Point	NED	Difficult to switch context from one Board to another in cybersecurity when there is no common framework or approach
C#12	Aspiration	NED	Cybersecurity risk discussions need to be part of the broader risk and controls framework.

Table 38: Core Concerns for board cybersecurity governance

6.3 Framework Validation – Expert Evaluation Workshop

The aim of the Expert Evaluation Workshop was to explain the BCGF in context of the RQ it was addressing, in making it easier for NEDs and CXOs to better govern cybersecurity, in the context of the 7 foundational models in the BCGF. Through this, participants provided initial feedback on the appropriateness of the models in the BCGF and the extent to which they should appear in such a framework or not. Further participants provided feedback on the nature of any guidelines that should be developed to assist in the implementation of the models. The expert evaluation workshop was attended by 20 participants, some of whom were involved in the one-on-one interviews, along with staff with cybersecurity expertise from academic institutions, and subject matter experts from consulting organizations that provide cybersecurity advisory services. Pre-reading documentation was sent to participants covering the context, challenge, and a high-level overview of the BCGF. The questions detailed in Figure 39 were sent to the participants to consider.

Ahead of the workshop please consider

1. Generally, is there an inherent challenge in Board/CXO oversight of cybersecurity ?
2. If so, does a lifecycle approach to this assist in some regards?
3. Are the 7-elements in the BCGF on page 6 adequate for providing further assistance?
4. What would you add/remove from the 7-elements?

A walkthrough of the 7-elements in the BCGF will be conducted in the workshop, followed by an online questionnaire to seek your feedback.

Thank you

Figure 39: Pre-workshop considerations for participants

The structure of the workshop has been previously outlined in the Research Method and Approach, Section 4.6.6. The workshop consisted of a walkthrough of the problem statement and then gave a clear framing of the intent of the workshop as outlined in Appendix 8.6. The workshop then explained the high-level BCGF (as outlined in Chapter 5) and detailed the business scenarios under which each of the 7 models would be applied and how this would typically occur. Following this run-through, participants were able to ask clarifying questions and also provide qualitative feedback on the BCGF and underpinning models. This feedback helped to inform the various dimensions of BCGF models, such as the implementation guidelines, inputs, and outputs, as detailed in Table 30 (BCGF Models Metadata). Thereafter, participants were asked to complete the next stage of the expert evaluation, which is the online survey to gain quantitative feedback. This is detailed in the next section.

6.4 Framework Validation – Expert Evaluation Survey

6.4.1 Survey Summary

As detailed in Chapter 4.6.7 (Research Method), the expert evaluation survey was anonymous and only available to the attendees of the workshop which explained the nature of the BCGF through the use of scenarios. It was structured into the dimensions and approach outlined in Section 4.6.7 (Expert Evaluation Survey), with evaluation criteria covering completeness, importance, relevance and practicality of the BCGF. Of the 20 experts attending, 15 completed the survey, including providing some verbatim feedback in qualitative form. The results of the survey helped to evaluate and improve the BCGF, as detailed in the following sub-section.

6.4.2 Results Summary

The survey provided constructive feedback on the BCGF. The number of responses from NEDs who govern cybersecurity posture overall and the responses from CIOs/CISOs/advisors who drive implementation were similar as shown in Figure 40. Those in the 'other' category included Heads of Security, who did not use the CISO title. There was a broad balance of roles that govern the state of cybersecurity (or advise on this), namely Consulting & Advisory and NEDs, and those who are responsible for its implementation (the other roles).

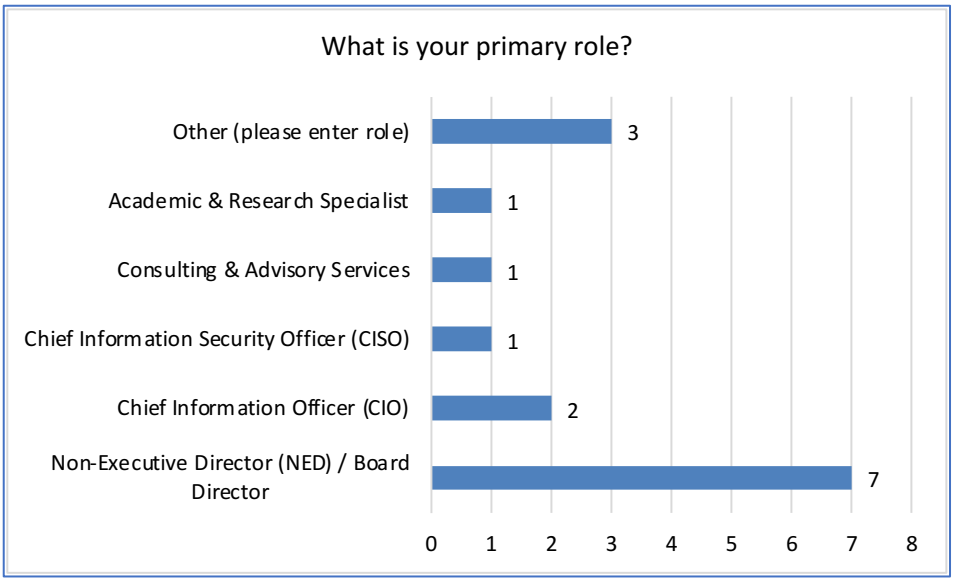

Figure 40: Roles in expert evaluation survey

In the first section of the survey, general questions were asked to capture the overall feedback on the completeness of the BCGF. This covered the approach to scope, lifecycle, and assurance. The responses provided confirmation on these dimensions being of value to the experts, with most responses agreeing or strongly agreeing on these dimensions being covered well. Only one response was neutral on assurance being relevant for the BCGF. See Figure 41 for specific responses on the three overarching questions.

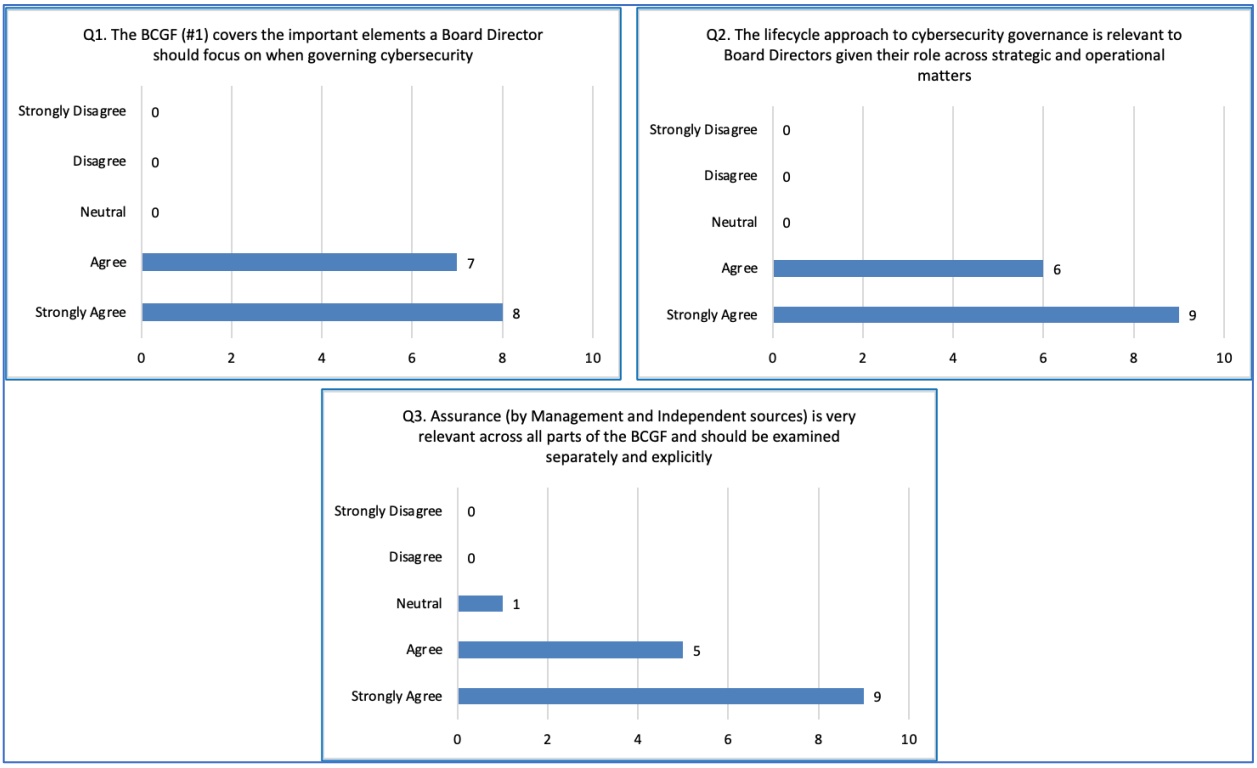

Figure 41: Evaluation of completeness of BCGF

Each of the 7 foundational models were then evaluated by the expert group in terms of the importance, relevance, and practicality of the models. The responses on the importance are shown in Figure 42. As can be seen, there was positive feedback on the models being important for the Board Director, with only 1 response being neutral (on the Assets Model). No responses indicated disagreement.

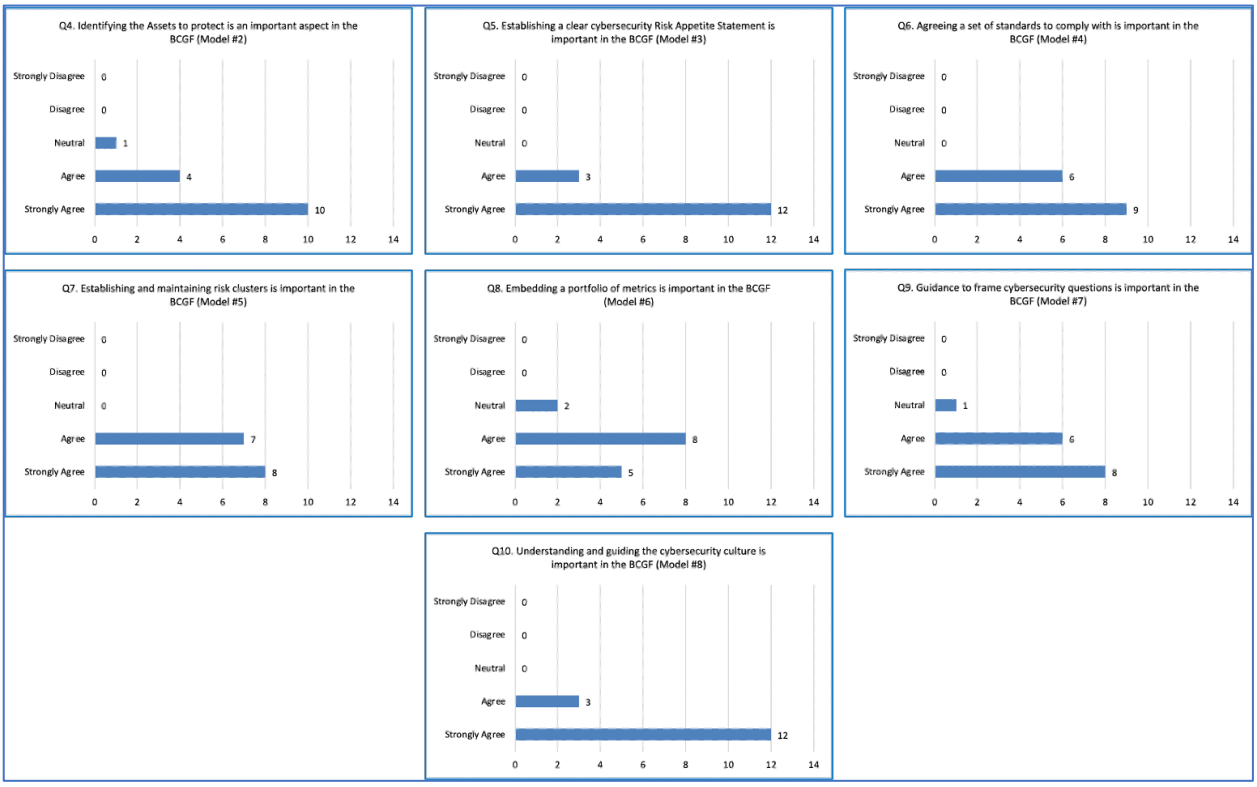

Figure 42: Evaluation of importance across BCGF models

The next aspect included feedback on the relevance of the BCGF models to Board Directors. As seen in Figure 43, there was strong confirmation on this dimension as well, with the majority of responses being agree and strongly agree. No responses indicated disagreement.

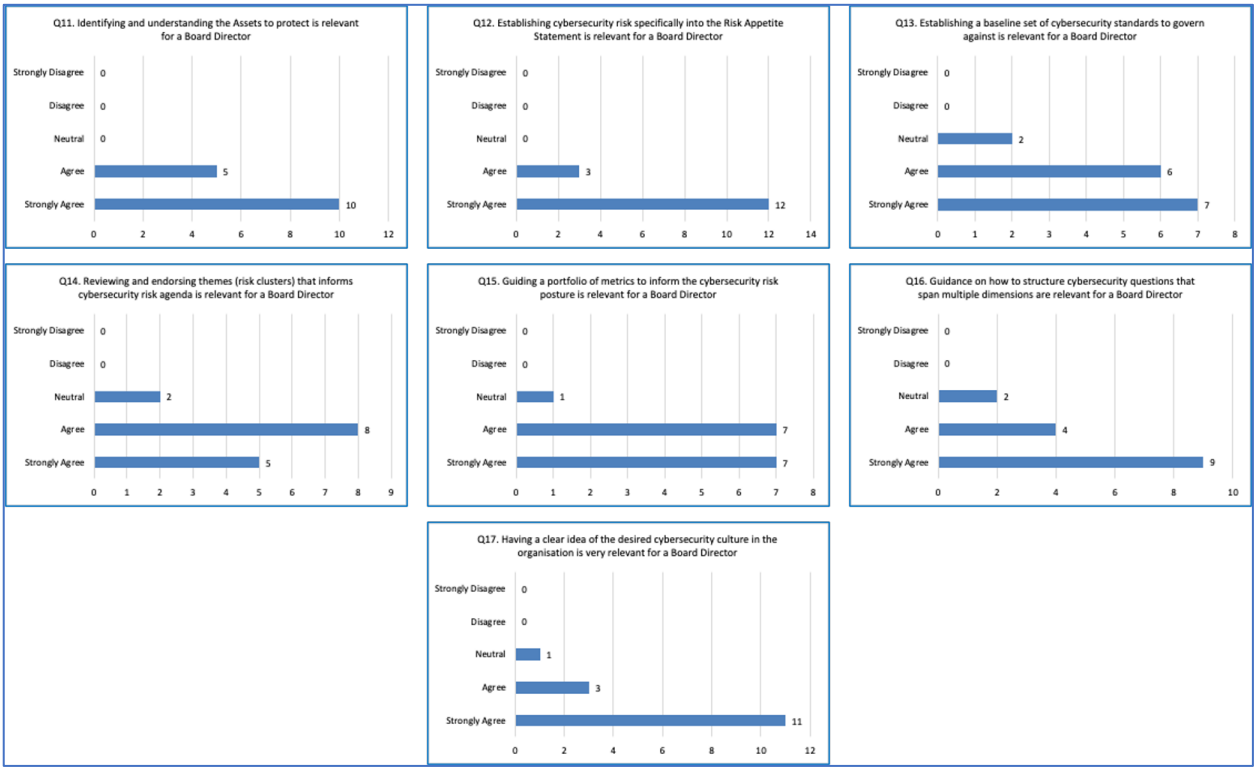

Figure 43: Evaluation of relevance across BCGF models

Practicality was accessed across four dimensions that represented the ease of understanding the framework, the ability to implement the models, and their usefulness from a practical perspective. The results for this are depicted in Figure 44. No responses indicated disagreement.

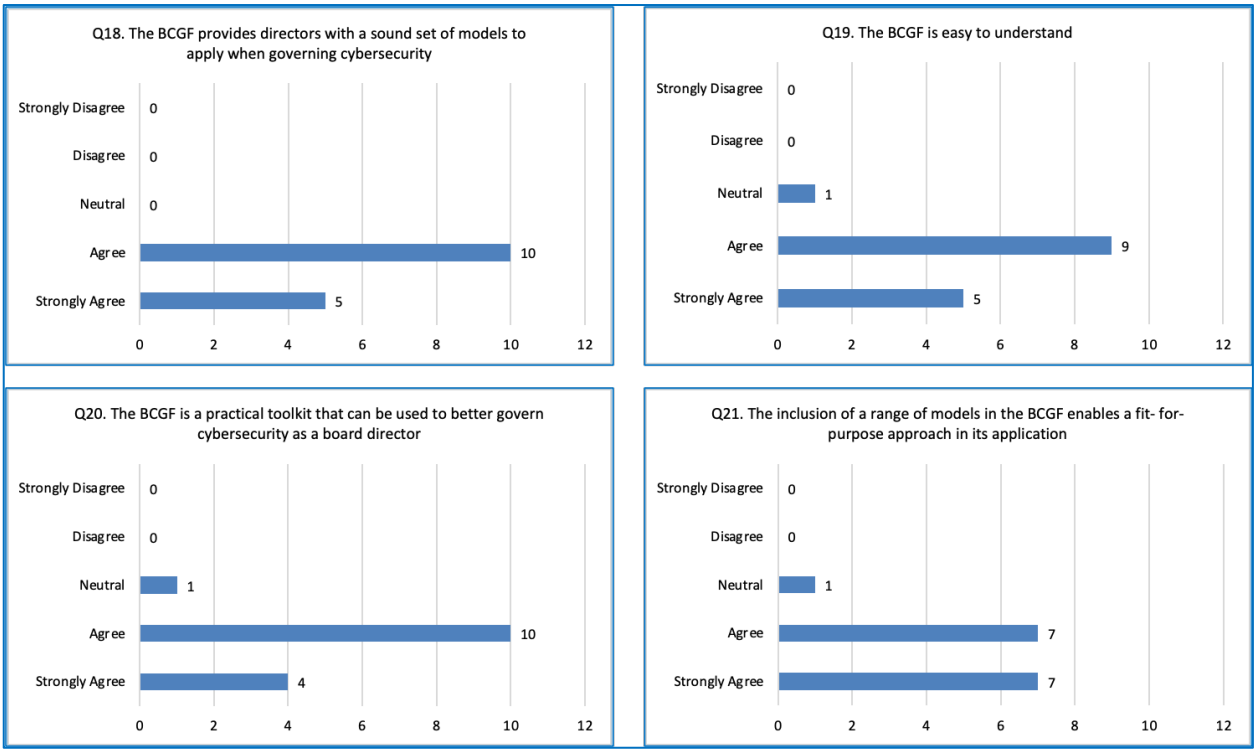

Figure 44: Evaluation of practicality of BCGF models

The final question related to which models the experts would remove from the BCGF. The results from this are depicted in Figure 45. Of the 15 experts who responded, only a very small minority felt any models should be removed, namely 2 experts (0.13% of responses) flagged the Questions model for removal, and 1 each (0.07% of responses) for the removal of the Metrics and Risk Clusters models. This feedback was not large enough to justify removal and was likely reflective of a greater level knowledge amongst some directors in asking questions in general. This is appropriate, as the model focusses on questioning related to cybersecurity and therefore offers supplementary guidance in this area on top of the regular questioning skills NEDs have on general business matters.

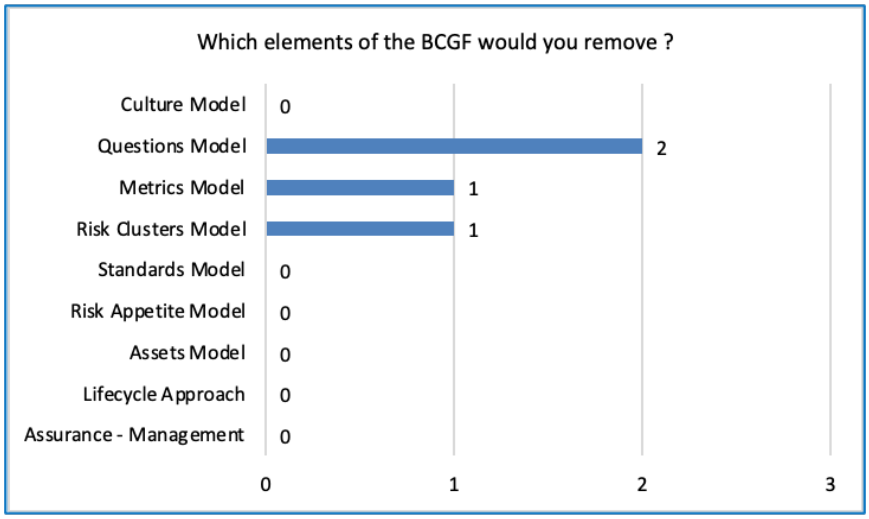

Figure 45: Evaluation of models to remove from BCGF

If we take each of the quantitative questions in the survey (Q1 to Q21 - see Appendix 8.7.2) and tabulate the responses, we see a favourable confirmation of the models meeting the stated evaluation criteria as

per Table 39. As can be seen, 95% of responses agree or strongly agree with the BCGF positively meeting the evaluation on completeness, importance, relevance, and practicality dimensions.

	Completeness			Importance							Relevance							Practicality				Rating Total	Percentage
Rating	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21		
Strongly Disagree	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.00%
Disagree	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.00%
Neutral	0	0	1	1	0	0	0	2	1	0	0	0	2	2	1	2	1	0	1	1	1	16	5.08%
Agree	7	6	5	4	3	6	7	8	6	3	5	3	6	8	7	4	3	10	9	10	7	127	40.32%
Strongly Agree	8	9	9	10	12	9	8	5	8	12	10	12	7	5	7	9	11	5	5	4	7	172	54.60%
																						315	

Table 39: Overall scores for questions in survey

For further insights, the average scores for completeness, importance, relevance, and practicality dimensions are examined in a clustered column graph. As shown in Figure 46), we see the clustering of positive feedback in the agree and strongly agree responses as depicted through all four evaluation dimensions. Further examination of this reveals a right-sided positive skewness of 0.68 for the ratings (strongly disagree, disagree, neutral, agree and strongly agree).

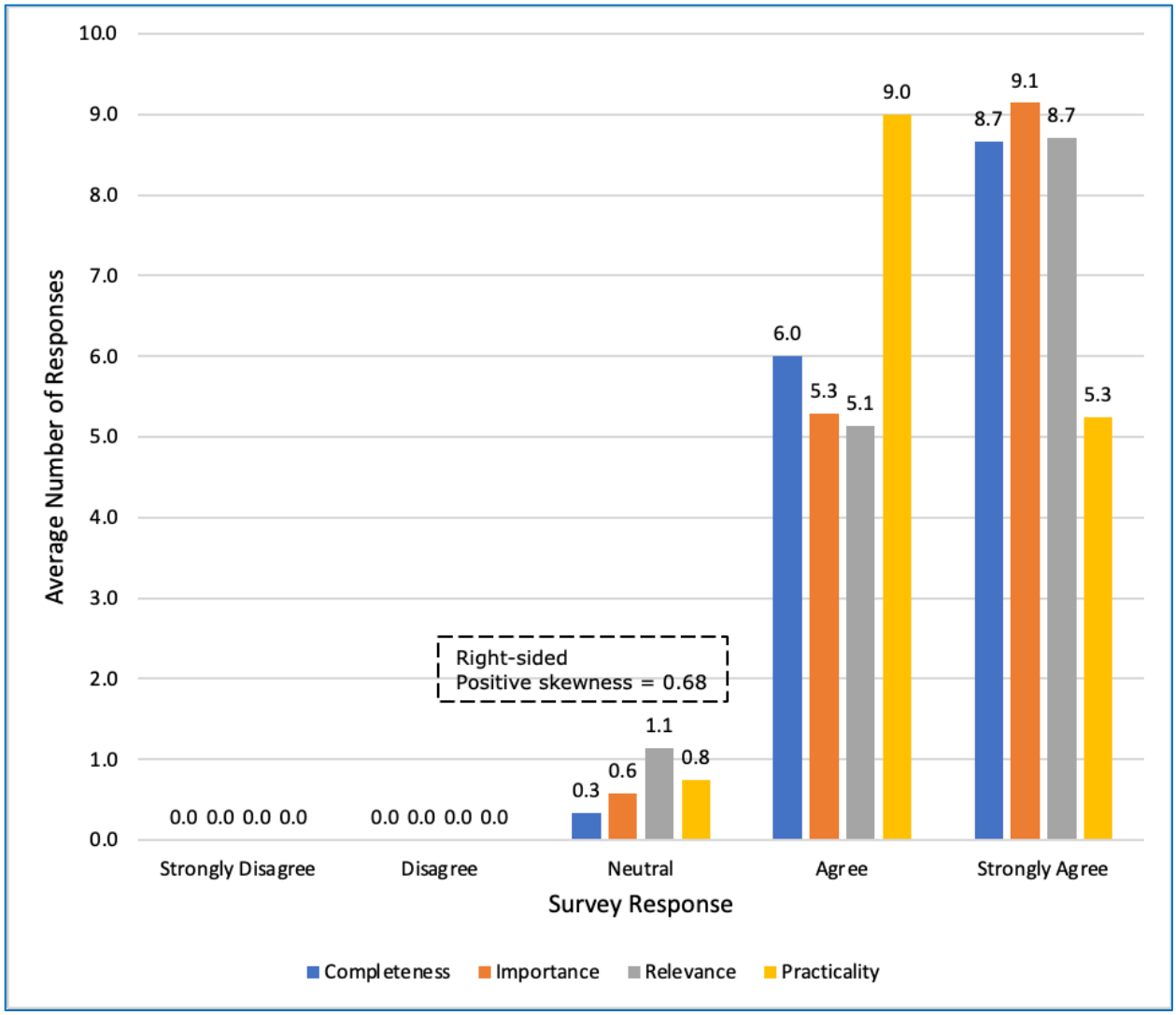

Figure 46: Overall ratings in evaluation dimensions

6.4.3 Statistical Analysis

The survey results are analysed using the chi-squared test on the BCGF evaluation results from Q1 to Q21, which cover the evaluation dimensions of completeness, importance, relevance and practicality. The key formulae, hypothesis, and variables are shown in Table 40.

Formulae
Chi-square goodness of fit test: $X^2 = \sum \frac{(O-E)^2}{E}$ O is the observed frequency E is the expected frequency (assumed to be equal (3) across all questions and ratings, i.e. 3 responses for each of the 5 ratings for a question, based on 15 respondents)
Hypothesis
H_0 – Null hypothesis. The BCGF and the evaluation criteria are not associated.
H_a – Alternative hypothesis. There is positive association between BCGF and the evaluation criteria.
If X^2 value is greater than (cv), then the difference between the observed and expected distributions is statistically significant. This data allows rejection of H_o and provides support for H_a. If X^2 value is less than (cv), then the difference between the observed and expected distributions is not statistically significant. This data doesn't allow rejection of H_o and doesn't provide support for H_a.
Variables
Degrees of freedom (df) = 14 (# respondents 15)
Test of significance $(\alpha) = 0.05$
Critical value (cv) = 23.6850 (from chi-squared distribution table)

Table 40: Key variables for chi-square test

The chi-square test is applied to each of the evaluation criteria. If we examine the completeness criteria and the associated analysis shown in Table 41, we see that the chi-square for this is 66.22. This is greater than the critical value (cv) of 23.6850, and therefore this allows rejection of the null hypothesis (H_0) and provides support for (H_a) which means there is positive association between the BCGF and the completeness criteria.

Completeness (Q1 - Q3)					
Rating	**Observed (O)**	**Expected (E)**	**O-E**	**(O-E)2**	**(O-E)2 / E**
Strongly Disagree	0	9	-9	81	9.00
Disagree	0	9	-9	81	9.00
Neutral	1	9	-8	64	7.11
Agree	18	9	9	81	9.00
Strongly Agree	26	9	17	289	32.11
				X^2 =	66.22

Table 41: Chi-square test on completeness criteria

If we examine the importance criteria and the associated analysis shown in Table 42, we see that the chi-square for this is 156.00. This is greater than the critical value (cv) of 23.6850, and therefore this allows rejection of the null hypothesis (H_0) and provides support for (H_a) which means there is positive association between the BCGF and the importance criteria.

Importance (Q4 - Q10)					
Rating	**Observed (O)**	**Expected (E)**	**O-E**	**(O-E)2**	**(O-E)2 / E**
Strongly Disagree	0	21	-21	441	21.00
Disagree	0	21	-21	441	21.00
Neutral	4	21	-17	289	13.76
Agree	37	21	16	256	12.19
Strongly Agree	64	21	43	1849	88.05
				X^2 =	156.00

Table 42: Chi-square test on importance criteria

If we examine the relevance criteria and the associated analysis shown in Table 43, then we see that the chi-square for this is 136.95. This is greater than the critical value (cv) of 23.6850, and therefore this allows rejection of the null hypothesis (H_0) and provides support for (H_a) which means there is positive association between the BCGF and the relevance criteria.

Relevance (Q11 - Q17)					
Rating	**Observed (O)**	**Expected (E)**	**O-E**	**(O-E)2**	**(O-E)2 / E**
Strongly Disagree	0	21	-21	441	21.00
Disagree	0	21	-21	441	21.00
Neutral	8	21	-13	169	8.05
Agree	36	21	15	225	10.71
Strongly Agree	61	21	40	1600	76.19
				X^2 =	136.95

Table 43: Chi-square test on relevance criteria

If we examine the practicality criteria and the associated analysis shown in Table 44, then we see that the chi-square for this is 85.50. This is greater than the critical value (cv) of 23.6850, and therefore this allows rejection of the null hypothesis (H_0) and provides support for (H_a) which means there is positive association between the BCGF and the practicality criteria.

Practicality (Q18 - Q21)					
Rating	**Observed (O)**	**Expected (E)**	**O-E**	**(O-E)2**	**(O-E)2 / E**
Strongly Disagree	0	12	-12	144	12.00
Disagree	0	12	-12	144	12.00
Neutral	3	12	-9	81	6.75
Agree	36	12	24	576	48.00
Strongly Agree	21	12	9	81	6.75
				X^2 =	85.50

Table 44: Chi-square test on practicality criteria

In conclusion, the ratings indicate that 95% of responses agree or strongly agree that the BCGF meets the evaluation criteria. The results have a right-hand positive skewness of 0.68 as shown in Figure 46. Further, the chi-square goodness of fit test demonstrates rejection of the null hypothesis (that the BCGF

and evaluation criteria are not associated). This implies support for the alternative hypothesis (that there is positive association between the BCGF and the evaluation criteria). In this case, the difference between the observed and expected distributions is statistically significant.

6.4.4 Qualitative Analysis

The expert evaluation survey captured qualitative feedback from participants for two questions as detailed in Table 45.

Question#	Question
Q23	What other elements would you add to the BCGF?
Q24	What other improvements would you like to add to the BCGF?

Table 45: Qualitative questions in expert survey

The responses from the participants to these qualitative questions are provided in Table 46, including details on whether the feedback has been included in the BCGF. As can be seen, the feedback overall is positive/neutral, with some improvement opportunities that have recognised and incorporated.

Question#	Feedback#	Participant Feedback	Feedback Type	BCGF Models	Comments	Action Taken
Q23	F#1	QA might be part of standards	Positive	Standards Questions	Quality assurance is an inherent part of compliance to the stated standard(s) and is already part of Standards and Questions Models. For Board Directors, the BCGF provides guidance on how to select the appropriate standards. The reporting on compliance to these is a management responsibility which is not the target audience for the framework. Assurance to the selected standard is covered in the Questions Model which gives guidance to directors on the breadth and depth of questions to ask to seek assurance.	Not Incorporated (No action required from feedback)
Q23	F#2	Boards should not be involved with operational aspects of cyber but provide oversight. Need a way to ensure enough attention is given to business continuity and recovery.	Improvement	Assets Risk Appetite	Already inherent in these models, however the operational resilience dimension has been explicitly added in the Risk Appetite Model, with associated guidelines on usage. This covers cybersecurity impacts to business continuity and recovery.	Incorporated (Added new dimension)
Q23	F#3	Planning and practice cyber simulation to build muscle memory of the organisation.	Neutral	Culture	Simulations are already detailed in the Culture Model as a mechanism that can be used to not just create awareness, but also strengthen culture on the impacts and consequences from a cybersecurity incident and how to respond. Culture is directly related to the 'muscle memory' of the organisation.	Not Incorporated (No action required from feedback)
Q23	F#4	Business continuity is critical. The other point raised is around technical controls which are extremely important (which is the basis for the Essential 8).	Improvement	Assets Risk Appetite	As per F#2, the business continuity is inherent in existing models, however the Risk Appetite Model has been enhanced as a consequence of the feedback.	Incorporated (Added new dimension)
Q23	F#5	Investment model.	Neutral	Assets Risk Appetite	Aspects related to the impact of cybersecurity posture/events to share price and revenue are covered in the Risk Appetite Model. Inherent in this is that the trade-off in costs versus value/risk is an understanding of the investment required. Such ROI and risk reduction are covered in the implementation guidelines of the Assets and Risk Appetite Models.	Not Incorporated (No action required from feedback)
Q23	F#6	Identity model.	Improvement	Assets	Typically, identity management (authentication and authorization) is an implementation aspect for CIO/CISO roles. However, the Assets Model has been enhanced to cover the need to specify special requirements an organization or industry sector requires in identity management. This includes aspects such as separation of duties, multi-factor	Incorporated (Added into People dimension)

Question#	Feedback#	Participant Feedback	Feedback Type	BCGF Models	Comments	Action Taken
					authentication, or special police/security clearances for people.	
Q23	F#7	I would aim for a continual assurance model.	Positive	Questions	Covered in the assurance part of the Questions Model, where this can be assurance from management or independent sources.	Not Incorporated (No action required from feedback)
Q23	F#8	I think Ppople need to be included in the crown jewels.	Improvement	Assets	People are an inherent part of business processes in the Assets Model, in terms of their roles and responsibilities. However, this has been now added as a separate asset type, from the perspective of protecting the people online when they conduct business.	Incorporated
Q24	F#9	Board scenario testing and war games.	Neutral	Culture	Already covered in F#3.	Not Incorporated (No action required from feedback)
Q24	F#10	Find a way to include resilience, response, and business operations continuity. We are doing work in this area at MIT.	Improvement	Assets Risk Appetite	Already covered in F#2 where improvements have been applied to the BCGF.	Not Incorporated (No action required from feedback)
Q24	F#11	A clearer way to right fit the model dependant on industry, regulatory, maturity etc.	Neutral	BCGF All	Already present in the implementation guidelines which are part of each model in the BCGF, as documented in Chapter 5. These outline the dimensions to tailor for making the models fit-for-purpose. The BCGF has been intentionally left generic to aid application and instantiation across industries and various maturity levels. Each model is standalone and has dimensions that can be applied as is or tailored.	Not Incorporated (No action required from feedback)
Q24	F#12	Given it is a matter of when, not if, a cyber-attack occurs, the response is imperative and will have the most impact on the value of the organisation. Defensible.	Positive	Risk Appetite	Agree with the statement. This is covered in the Risk Appetite Model. The model covers the need to understand the impact to the organisation, and establishing the right risk appetite, protection levels, and response levels.	Not Incorporated (No action required from feedback)
Q24	F#13	My “neutral” on Practical was really related to the baseline level of understanding that may be required for NEDs to engage with the framework. My slight concern is that this framework may become the domain if the ‘cyber expert’ or the	Neutral	Risk Clusters	The feedback relates to the Risk Clusters Model, which is intended to help crystallise not just the top cybersecurity risks for the organization, but also practically inform the director education curriculum. This approach, as outlined in the implementation guidelines for this model in Chapter 5, helps	Not Incorporated (No action required from feedback)

Question#	Feedback#	Participant Feedback	Feedback Type	BCGF Models	Comments	Action Taken
		'digital native' directors - similar to the way that finance became the domain of the token accountant in the 80s… hope that makes sense… There may need to be a cyber literacy part (perhaps as part of the Establish phase). As I am typing this - someone is talking about including a Director Duty lens - Hanrahan handbook may help with a brief note on to whom the duty is owed… there is a good section on community and reputation.			directors to focus on a narrower scope of education to improve understanding and cybersecurity literacy. Overtime, knowledge of cybersecurity will improve due to the focus on just-in-time education that is informed by external and internal risks across short- and medium-term horizons.	
Q24	F#14	Consider aggregating Standards and Metrics, and prioritising the core models, starting with Risk Appetite, then Culture.	Neutral	BCGF All	The BCGF has been developed in a manner that allows optionality in use of the models during different stages of the cybersecurity lifecycle. In research conducted with participants, the importance of this and being able to adapt the BCGF to specific industry sectors and organization maturity was important. This would allow a fit-for-purpose approach. As such, models were normalised into usage patterns across the lifecycle, and not aggregated into larger artefacts. Similarly, the priority or sequence of usage was not embedded in the BCGF to enable instantiation in the manner the organization required according to its priorities and cybersecurity maturity.	Not Incorporated (No action required from feedback)
Q24	F#15	Financial prioritisation - what is the appropriate level of investment, how much is enough?	Positive	Assets Risk Appetite	The discussions on investment levels and desired risk acceptance are already outlined in the implementation guidelines of the Assets Model (determining what to protect) and then the Risk Appetite Model (what the desired level of protection and operational resilience should be, and then the cost of this). Prioritisation is an outcome from application of these models.	Not Incorporated (No action required from feedback)
Q24	F#16	Very specific on some elements in the RAS and response and recovery try from the Board that help to drive the initiatives within Management - expectations and importance at the Board level on how a cyber incident will be responded to.	Positive	Risk Appetite Culture	The need to be specific in multiple dimensions in the Risk Appetite Model is critical as that is where the Board can set expectations of management. This includes the necessary expectations on response in the event of a cybersecurity incident.	Not Incorporated (No action required from feedback)
Q24	F#17	I have no doubt that many organisations that have experienced a cyber security event spend more on it now that they did previously. Given many	Positive	Assets Risk Appetite	The Assets and Risk Appetite Model represent the themes in this feedback. It is here that the discussion on cost/investment needs are weighed up with expectations on protecting the	Not Incorporated

Question#	Feedback#	Participant Feedback	Feedback Type	BCGF Models	Comments	Action Taken
		Boards don't have CIO representation or may have low tech, digital and cyber experience how do they know the appropriate investment profile for this space is being met. It's one thing to spend on remediation after the event but what about investment in what is a highly contestable space - and probably more so in the private sector than government.			critical assets, and also the desired levels of operational resilience from cybersecurity events. The comment reinforces the importance of this discussion and the magnitude of the investment that may be necessary to attain the risk appetite.	(No action required from feedback)
Q24	F#18	Document examples of it can be applied to various industry sectors.	Positive	BCGF All	Implementation guidelines form part of the final BCGF and several mechanisms to tailor the models for specific situations are presented.	Not Incorporated (No action required from feedback)
Q24	F#19	1. I am not sure that I would separate assurance between management and independent- good management is obtaining independent assurance. 2. It would be helpful for the Board to have a range of what appropriate spend quantum might be for an organisations size and maturity. E.g. (these are made up numbers) Low maturity org might be 15% of revenue to move to medium maturity, 20% to move to high. Could be percentage of assets under management - either way it needs to meet the would a reasonable person in the same situation with the same information have made a similar decision.	Neutral	Questions Risk Appetite	The separation of assurance into management and independent was carried out to explicitly show the difference. Interviewees did mention that in many cases they rely on management assurance alone, and in the case of cybersecurity risk this may not offer the depth of review in detail controls. The Questions Model provides an explicit decision point that allows either style of assurance, depending on the situation and risk of the matter. The benchmarks on quantum of spend are areas that typically would be discussed in the Risk Appetite Model. These can be derived from relevant research organisations (e.g. Gartner), or consulting companies.	Not Incorporated (No action required from feedback)
Q24	F#20	This framework seems to have elements of global application to so many risks/challenges facing business. I think it needs to contemplate how it would fit into other pre-existing frameworks in business or be used as a basis for a remodelling for the business. Would like to understand how this framework would be communicated across the business.	Positive	BCGF All	Agree, the right way to embed this is into the existing processes and frameworks the Board has in place that can be leveraged. For example, the Board Risk Framework should have linkages to BCGF models that can be applied and then the output is used to inform the overall organization Risk Appetite Statement. This embedding or implementation of the BCGF and models is covered in Chapter 5.	Incorporated (No action required from feedback)

Table 46: Qualitative comments in expert survey

A summary of the comments is presented in Table 47.

Dimension	Number
Positive Comments	8
Neutral Comments	7
Improvement Opportunity Comments	5
BCGF Models Covered	Assets, Risk Appetite, Risk Clusters, Standards, Questions, Culture, Overall BCGF.

Table 47: Summary of qualitative comments

6.5 Overall Framework Evaluation and Cross-Reference Check

One additional evaluation step of the BCGF includes a cross-reference between the BCGF models and the expert concerns expressed during the one-on-one interviews (as summarised previously in Table 38). This mapping is shown in Table 48 and further reinforces the contribution of the BCGF artefacts produced through the adopted DSR approach (and supplemented with GT techniques). The line of sight between concerns and the area of the BCGF in which they are addressed is clear.

BCGF Model	Concerns enabled (see Table 38 for list of Concerns)
Overall Framework (BCGF)	C#7, C#11, C#12, C#6
Assets Model (section 5.5)	C#3, C#6, C#10, C#4, C#5
Risk Appetite Statement Model (section 5.6)	C#4, C#5, C#6, C#12, C#2, C#3, C#8, C#9, C#10
Standards Model (section 5.7)	C#9, C#8
Risk Clusters Model (section 5.8)	C#1, C#12
Metrics Model (section 5.9)	C#8, C#1, C#6
Questions Model (section 5.10)	C#2, C#1
Culture Model (section 5.11)	C#11, C#12

Table 48: Mapping of BCGF models to interviewee concerns

6.6 Summary

This chapter detailed the results and insights gleaned from the interviews and the outcomes from the validation of the proposed BCGF via the expert evaluation workshop and expert evaluation survey. Complementary techniques were used to evaluate the BCGF, including the expert evaluation workshop to allow questions and comments, the expert evaluation survey to quantitively measure the usefulness of the survey for NEDs, and finally reconciliation of the concerns raised by the NED/CIO/CIO interviewees to the artefacts in the BCGF that address these. Further, data visualisation, including chi-square analysis and skewness considerations reinforced the validity of the BCGF being able to assist the NED and CXO stakeholders. The next chapter discusses the BCGF and the evaluation results and concludes with options for further research.

7 Discussion and Conclusion

7.1 Introduction

This thesis proposed the BCGF to address an important research gap and practical need for Board level cyber governance. The proposed framework has been developed and evaluated using the well-known DSR method. The previous chapter detailed the results and insights gleaned from the interviews, the outcomes from the validation of the BCGF via the expert evaluation workshop and the expert evaluation survey. It also covered complementary techniques to further evaluate the BCGF, such as the synthesis of feedback using statistical analysis to demonstrate how the BCGF meets the evaluation criteria, and a cross reference to show how concerns raised by interviewees were met by models in the BCGF. This chapter concludes and demonstrates that the BCGF is novel and addresses an important research problem to assist Board Directors and Senior Executives better govern cybersecurity. Finally, it also details implications, risks and key learnings including future research directions.

7.2 Research Context and Validity

This section summarises the discussions on the context of the research, in terms of the challenges Board Directors and Senior Executives face when governing a field such as cybersecurity, and the need to address this problem area, given the growing dependency on digital platforms. This discussion is based on the perspective of importance of the research, the audience targeted, and research validity.

7.2.1 Importance

The importance of managing cybersecurity risk has been covered previously with relevant references and discussion in Chapter 1 – Introduction (Section 1.2) and Chapter 2 – Research Background and Problem (Section 2.6). These discussions highlight the growing need to manage cybersecurity risk in the digital economy, as threats have increased in sophistication and volume. In addition, consumers have become more reliant on online digital services (ACSC, 2022; Li & Liu, 2021), and this has in turn, required organizations to expand their online platforms, and strengthen them to be more resilient to cybersecurity threats. Many of these platforms provide services 24x7 due to the growth in demand and expectations from customers and stakeholders, and this brings complexity in solution design and operations (Gielens & Steenkamp, 2019; Guthrie et al., 2021). The negative consequences of cybersecurity incidents impact not just the organization in question, in terms of reputation and financial loss, but also have an ongoing impact on consumers who have to manage any theft of their personal data from breaches (APRA, 2023; OPTUS, 2023). In some cases, consumers have taken legal class actions against organizations that have failed to secure their data adequately as seen recently in the Medibank and OPTUS breaches in Australia (Gordon, 2023a, 2023b). In many jurisdictions and sectors, legal penalties have been imposed by regulators on executives and companies that do not adequately govern the posture of cybersecurity (ASIC, 2020; Haislip et al., 2021; Walton et al., 2021). This has more recently included fines and additional regulatory capital requirements in industries such as financial services (APRA, 2023; SCC/SEC, 2023). In addition to the growth of online digital platforms, and the increased focus of regulators for organizations to maintain their risk posture, the sophistication and volume of cybersecurity attacks has grown, placing increased requirements upon leaders (Li et al., 2019; Walton et al., 2021). New technologies available to attackers and the corresponding complexity in risk mitigation makes the task of protecting organizations and consumers even more difficult when it comes to technical know-how and obtaining assurance on the quality of the implementation of solutions and risk mitigants (Brown et al., 2017; Walton et al., 2021).

7.2.2 Audience

Overall accountability for the posture of cybersecurity risk sits with the Board of Directors in an organization, and in the case of government entities, there are equivalent state and/or federal leaders and governing bodies in place. Regulators (and shareholders) ultimately hold this level of leadership and are accountable for managing cybersecurity risk, amongst other risks (AICD, 2022a; AICPA, 2018; Anderson et al., 2017; Brown et al., 2017; CAQ, 2018; Dupont et al., 2023; Peppard et al., 2023; Proudfoot et al., 2023; Slapničar et al., 2023). This is further supported by more recent guidance from the AICD targeted at Board Directors in regard to how they should respond and recover in the event of a cybersecurity incident in their organization (AICD, 2024b). The Board of Directors rely upon management, in the form of various CXO roles such as CEO, CIO, CRO and CISO, to implement the desired controls whilst the Board remains accountable in an oversight role ongoing. It is in this oversight responsibility and the interface to CXO roles that a range of challenges exist for Board Directors and their confidence to fulfill this important accountability. This is seen in ASX/ASIC (2017) where only 50% of Boards were somewhat confident that their company was adequately secure against cybersecurity threats, only 34% of organizations had a cybersecurity risk appetite defined, and only 11% of Boards had a clear understanding of when and where the company's key information and data assets are shared with a third party. These levels of confidence are further reduced due to the increasing complexity in governing cybersecurity. An example of this complexity is regulatory change that now imposes responsibilities on Boards for risk arising from third-party organizations in the value-chain that supports their own organizations (APRA, 2019). In this scenario, Directors must have adequate oversight, assurance and governance of the cybersecurity posture of such third parties. Further, the ongoing innovation in technology brings new forms of cybersecurity attacks and also new solutions to mitigate these. This requires Directors to have a level of ongoing understanding of these areas to govern this complex and changing scenario effectively and with confidence (Brown et al., 2017; Walton et al., 2021). Finally, the academic and industry literature does not provide a consistent view of the definitions and dimensions of cybersecurity which, in turn, causes confusion with industry practitioners such as NEDs, CXOs and related risk/audit SMEs, further adversely impacting their confidence. A case in point is Taherdoost (2022) who argues that whilst information security and cybersecurity cover similar dimensions, cybersecurity is limited to the cyber/internet domain, and therefore is a subset of information security. This view has been refuted by a number of authors who state the opposite, in that cybersecurity is broader and information security a subset (Rout, 2015; von Solms & van Niekerk, 2013). As such, the NED audience is hampered by a lack of frameworks and clarity in definition that is targeted at their specific governance accountabilities.

7.2.3 Research Validity

The research validity is demonstrated and evident from the systematic identification of a valid research problem, solution development and its evaluation using robust research method and underpinning techniques. For instance, this research identified a gap in the existing academic literature targeted at the NED audience in a language and at a level they can understand and apply. For example, in Chapter 2 - Research Background and Problem - Section 2.5 (Table 11), in a review of 9 industry cybersecurity artefacts (standards / guidelines), the target audience is primarily a technical SME that implements cybersecurity. The NED and CXO roles are not well served. The literature review detailed in Chapter 3 resulted in only 86 papers from academic and industry sources being relevant to this audience. This was from an initial set of 3,928 papers from academic sources and 1,001 from industry sources. Of the 86 that remained after skimming and filtering, only 63 were directly relevant to the NED stakeholder, with a focus centred only at a principle level. A summary of the coverage is depicted in Table 25 which details the number of candidate papers that fall into the framework of cybersecurity dimensions derived from the Cyber Security Governance Principles issued by the Australian Institute of Company Directors (AICD, 2022a). As shown, of the 6 dimensions, only the Leadership and Stakeholder dimensions are covered by more than 50% of the candidate papers and these provide limited guidance for NEDs, other than principle-level coverage.

In addition to the Literature Review, as part of the research method, participant interviews with NED, CIO and CISO stakeholders who had expertise in multiple industry sectors were conducted, as detailed in Chapter 6 - Results and Evaluation. Interviewees expressed pain points or aspirations (collectively termed 'concerns') when it came to governing cybersecurity at a Board level (NED role) or providing assurance to a Board on cybersecurity posture (CIO/CISO roles). These concerns effectively represent gaps in artefacts or processes, but if addressed, can help to improve cybersecurity governance at a Board level. The concerns were further evaluated in the Expert Evaluation Workshop, where the importance of the problem statement and the need to target the NED audience was discussed and confirmed. Table 49 shows the concerns as originally detailed in Table 38 in Chapter 6 (Results and Evaluation), where of the 12 major concerns, 10 of these stem from NEDs (responsible for overall governance), whilst the remaining 2 are from CIO/CISOs (responsible for implementation and provision of assurance). The concerns undeniably point to the need for a cybersecurity framework for use by Boards in their interactions with CXOs who are responsible for the implementation of cybersecurity.

Concern #	Perspective From	Description of Concern / Gap
C#1	NED	Timely education and training based on topics informed by internal and external risk scenarios or events.
C#2	NED	Techniques to question the state of cybersecurity in a generic way so that unknowns are identified and understood more easily.
C#3	NED	Understand the scope of the organisation's assets, that are of highest importance for protection and cyber resilience.
C#4	CIO/CISO	Boards being unable to define the risk appetite for cybersecurity incidents, and where it exists, it is vague and not informing.
C#5	NED	Risk/Cost analysis of cybersecurity posture is not detailed clearly in risk discussions with management.
C#6	CIO/CISO	Never enough time is allocated to review and discuss cybersecurity posture with the Board.
C#7	NED	Understanding cybersecurity in terms of the lifecycle would assist in focus and narrowing down discussions to specifics.
C#8	NED	Cybersecurity metrics are not meaningful, difficult to ascertain if they have the right breadth and depth; trends cannot be easily seen.
C#9	NED	Not clear on which standard is appropriate for compliance and the rationale for this is not presented in an independent manner.
C#10	NED	Executives rarely present a view of the criticality of various assets (systems, data, people, or process) to enable a cost/risk focus.
C#11	NED	Difficult to switch context from one Board to another in cybersecurity when there is no common framework or approach
C#12	NED	Cybersecurity risk discussions need to be part of the broader risk and controls framework.

Table 49: Summary Concerns from interviewees

The RQ is based on determining the nature of such a framework, in order to assist Board Directors and Senior Executives better govern cybersecurity. This is detailed in Section 2.7 (Research Question) and in Section 2.8 (Research Aims, Objectives and Deliverables), where the research sub-questions and deliverables are outlined. The factors that confirm and reinforce the validity of the research question (as per the references provided earlier in this section) are summarised in Table 50.

Validity#	Validity Factor	Description
V#1	Importance of Cybersecurity	Growth in digital economy and a need to drive confidence and trust in an environment of increasing regulation and cybersecurity attacks.
V#2	Accountable Audience	The NED stakeholder having limited coverage in literature from academic and industry sources, that is of a practical implementation level.
V#3	Interviewee Concerns	Identification of concerns (pain points and aspirations) by NED, CIO, and CISO audiences to improve Board cybersecurity confidence and effectiveness.
V#4	Expert Evaluation	Review and confirmation of concerns, and the need to address these to improve Board cybersecurity governance.
V#5	Concerns / Solution Cross-Ref	Cross reference of the concerns expressed by interviewees (NED/CIO/CISO stakeholders) to specific Models in the BCGF that address these.

Table 50: Factors confirming validity of the research question

7.3 Research Method and Evaluation

To answer the research question and determine answers to the sub-questions and associated deliverables outlined in Section 2.8, a comprehensive research method was followed. A conceptual view of this research method and steps to evaluate the artefacts is shown in Figure 47. The method and evaluation are discussed in the following sub-sections.

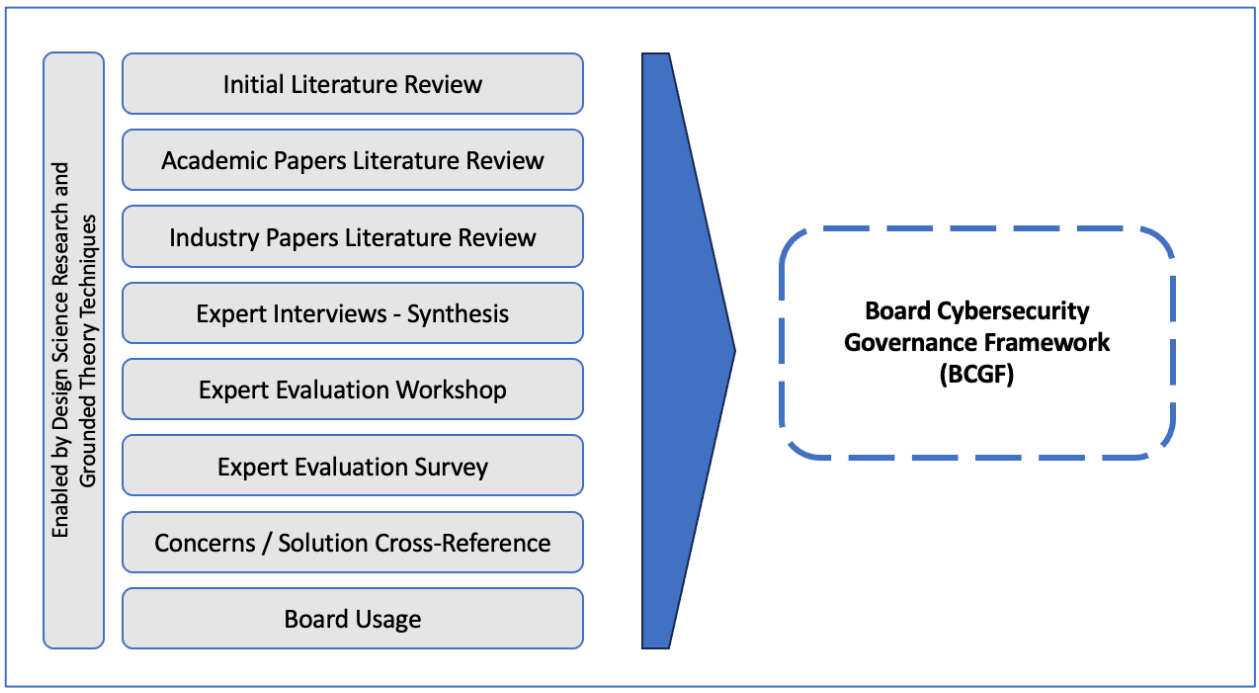

Figure 47: Conceptual view of research method and evaluation stages

7.3.1 Research Method

The research method was based on establishing sound academic rigour that enabled relevant industry experience/experts to provide critical and constructive input into the research process. The DSR approach, augmented with GT techniques to code and analyse concepts and derive insights was adopted, as detailed in Chapter 4 - Research Method. The research followed multiple complementary areas of focus that guided the design of artefacts and the evaluation of these, as detailed in Figure 19 where the application of the 7 DSR guidelines Hevner et al. (2004) is depicted to show the rigour and soundness of the process. Of specific note is the iterative manner in which an initial literature review, interviews, final literature review, and formulation of initial artefacts was carried out. This enabled viewpoints to be gleaned, the artefacts to be refined and the core concerns of the interviewees in terms of pain points and aspirations to be collected, which represented the requirements for any resultant framework to address the concerns. As such, the research method to inform and formulate the design

of the BCGF has soundness in academic rigour and industry input. Following the design stage, focus shifted to the evaluation stage, as per the DSR method.

7.3.2 Evaluation

The evaluation phase started with the Expert Evaluation Workshop where first an outline of the problem statement was given to the experts and a discussion ensued which indicated that there was agreement that this issue existed in industry and was worth researching and solving. Following this, a walkthrough of the resultant framework was carried out, including an overview of each of the models within this, and then the business scenarios under which NEDs could utilise these. Questions and comments at the end reinforced the soundness of the framework and some improvement opportunities (captured via the subsequent online survey). The next stage involved a detailed Expert Evaluation Survey that captured quantitative feedback on the evaluation criteria consisting of completeness, importance, relevance, and practicality of the BCGF. The results for this are detailed in Chapter 6 - Results and Evaluation. In summary, over 95% of the feedback was positive (agree and strongly agree) that the BCGF met the evaluation criteria. There was a right-sided skewness of 0.68 for ratings (strongly disagree, disagree, neutral, agree, and strongly agree). To complement this analysis, the chi-square approach was applied to confirm the hypothesis that there was positive association between the BCGF and evaluation criteria/results. Qualitative feedback was also captured to enable free form comments from the experts that allowed the further refinement of the BCGF. Finally, a cross-reference (depicted in Table 48) was conducted between the concerns (pain points and aspirations) raised in the one-on-one expert interviews and the models within the BCGF. This was done to ensure that the concerns interviewees expressed at the outset had been addressed by the final solution. The evaluation process clearly reinforced the applicability and suitability of the BCGF in addressing the RQ. The review and assessment of the BCGF gave strong support for the framework in terms of its validity as a tool that could assist Board Directors to better govern the cybersecurity risk.

7.4 Research Outcomes

The outcomes from the research address the RQ by providing a framework to help Board Directors and Senior Executives better govern cybersecurity. This framework has been designed and evaluated as summarised in the previous section, through the use of DSR techniques. These techniques assisted in bringing academic rigour and expert input to the design and evaluation stages of the solution. The solution, (consisting of the BCGF, its 7 foundational models, and detailed implementation guidelines), provide a fit-for-purpose solution that can be instantiated and adapted to the specific needs of an organization. Through this, not only has an important research gap been addressed, but also the BCGF offers practical application in the industry and an opportunity to further this research. The contribution of this research is now discussed in terms of implications to research, practice, policy, and industry.

7.4.1 Research Implications

The research applied the DSR method augmented with GT techniques. This was the core tenant that led to formulation of a framework with a basis on rigor in design and evaluation of the solution. It formed new knowledge for the NED that was absent in the prior literature, and therefore is novel in nature. Insights gleaned from the literature review of academic and industry sources (Chapter 3) confirmed the existing literature did not cover cybersecurity governance in relation to NEDs. This also highlighted the existence of principle-level guidance for this stakeholder group in a range of industry sources, but there was a distinct lack of detail on how such principles should be instantiated in organizations. Further, there was limited availability of models that could be used by NEDs to aid business-level cybersecurity risk discussions in a practical fact-based manner. However, interestingly, for the cybersecurity or risk SME there was an abundance of literature that included academic and industry papers, as well as many standards and guidelines targeted at the technical stakeholders. This was discussed in detail in Chapter 2 - Research Background and Problem, and Chapter 3 - Literature Review.

The literature review demonstrated that of the 4,929 papers identified across academic and industry sources, only 86 related to the NED and CXO audience, and only 64 of these were directly relevant to the RQ to determine which framework should be developed to help non-technical audiences, such as Board Directors and Senior Executives, better govern cybersecurity. As such, there were gaps in the prior literature relating to stakeholders who governed the posture of cybersecurity. These gaps were also confirmed through the use of GT techniques to synthesise NED concerns expressed in one-on-one interviews. When examining the set of 86 papers, as shown in Table 25 (Section 3.4) in Chapter 3 - Literature Review, the extent of coverage for NEDs in the academic and industry literature was low in assurance, benchmarking, and terminology, with regulation being medium. Table 51 depicts how the gaps in the prior literature have been addressed through new knowledge provided through the BCGF models.

	Cybersecurity Dimension	**Extent of coverage** High (H): >= 50% papers, Medium (M): 39-49%, Low (L): < 39%	**BCGF Models addressing Low / Medium Coverage Dimensions**
1	Leadership	H	Culture Model
2	Assurance	L	Assets Model, Risk Appetite Statement Model, Questions Model
3.	Benchmarking	L	Metrics Model
4.	Terminology	L	Risk Clusters Model
5.	Stakeholders	H	Questions Model
6.	Regulation	M	Standards Model

Table 51: BCGF models addressing gaps in literature coverage

The validity of this research outcome was enhanced by engaging highly experienced participants in interviews, an evaluation workshop, and an evaluation survey. The extent of experience in the final cohort of participants (as per Appendix 8.3) was an average of 34 years of cross-industry experience. Given the gaps identified for NEDs and the positive confirmation of the BCGF, this research contributes to new novel knowledge for NEDs that was absent in the prior literature.

In addition to the DSR methods, kernel theories have assisted in the analysis of data with a specific lens, and then models in the BCGF were refined and evaluated through the application of solutions to real-world problems (Möller et al., 2022; Vaishnavi & Kuechler, 2008). In particular, the “mechanisms of application” of the kernel theories detailed by Möller et al. (2022) have been applied in a range of research steps. Specifically, these have guided the formulation of an initial set of BCGF models that were evaluated by experts in the workshop, and also the characteristics of the resultant BCGF to a set of design principles. The authors argue the case that artefacts designed through DSR methods are enhanced through the application of kernel theories in various mechanisms that include the “analyze with lens”, “refine with”, and “evaluate with”. In particular, the Protection Motivation Theory is relevant to the BCGF Assets, Risk Appetite Statement, and Culture Models. This is where the personal motivations of NEDs and CXOs, in regard to the reputational damage caused by poor cybersecurity governance can have on them as individuals becomes an important cultural motivator aspect to factor for attention and focus (Menard et al., 2017; Schuetz et al., 2020). These authors also argue the case that Self-Determination Theory also plays a key role in the level of compliance users focus on if they believe this is a positive, desirable behaviour for their stakeholders. The BCGF models draw out and reinforce the constructs in these theories with a focus on the consequences which are negative if cybersecurity governance is poor but can be positive if models are applied to improve the effectiveness of relevant and activities and decisions.

Synthesis of the BCGF enables a number of key design principles to be abstracted, which also offers new novel insights on the nature of artefacts created through the application of the DSR method and GT techniques. These design principles can be seen as additional research insights that can guide the formulation of future solutions. A summary of the design principles abstracted from the BCGF are presented in Table 52.

Principle #	Design Principle	Design Principle Description	BCGF Linkage
1	Lifecycle	Consider the impact of a lifecycle approach to the constituents of the solution, in order to draw out applicability and relevance to stages.	BCGF takes a lifecycle view of cybersecurity governance, as each stage has relevance to the models and governance responsibilities for NEDs.
2	Adaptable	Design for adaptability in application, with optionality to instantiate in whole or part; anticipate tailoring requirements in design and evaluation.	Each model in the BCGF is standalone, and enables a fit-for-purpose implementation, to cater for varying levels of organizational maturity.
3	Behaviour	Understand the behaviour requirements and outcomes from the solution where multiple stakeholders are involved in its application.	The BCGF articulates the CXO roles that provide input into the use of models by NEDs, and also the desired behaviour from them in implementation.
4	Engagement	Design for horizontal use within a single target stakeholder group or be explicit if vertical integration to multiple downstream stakeholders is desired.	The RQ and BCGF has been targeted at the NED stakeholder explicitly, as a way to assist in cybersecurity governance.
5	Capability	Understand the skills and capability maturity of target users of the solution, so that guidance and level of detail is appropriate for them.	The Board of Directors are generally do not have deep technical background, and as such the solution has been designed with this in mind.
6	Structure	Architect the solution in a structure that enables various levels (or layers) of detail for flexibility and understanding.	A layered approach has been adopted with the BCGF, which is further segmented into 7 Foundational models for flexibility in usage.
7	Quality	Build quality steps in the framework that is realised in activities to apply it in practice, with expected inputs and outputs, and metrics of relevance.	The models in the BCGF each have clear inputs, outputs and implementation guidelines that guide quality into the implementation.
8	Meta Model	Design the scope of the elements in the solution intentionally upfront, so that its application is clear and practical.	The dimensions in the BCGF models are defined at the outset, including purpose, business scenario, stakeholders, etc. See Table 30.
9	Linkages	Embed linkages and relevance to other organizational processes into the solution, so as to make it relevant in application and practicality.	Each model in the BCGF has implementation guidelines that establish the linkages to processes or committees in the organization.
10	Scenarios	Provide practical scenarios to demonstrate the applicability of the solution in different situations, including how it can be used.	Business scenarios in the BCGF bring it to life in terms of the specific situation that could benefit from application of a model.

Table 52: Design principles abstracted from BCGF

7.4.2 Practice Implications

The structure of the BCGF (7 foundational models) enables the targeted application of specific models in certain stages of the lifecycle. In the course of the Expert Evaluation Workshop and other presentations, such an opportunity has been highlighted by other researchers and industry SMEs. As per section on List of Publications and Presentations, elements of the BCGF have been applied in practice in some Boards with a favourable response in usage. By way of example, in the event a Board is not aware of which assets it should be protecting as a priority, then the Assets Model in the BCGF becomes very relevant. For example, implementing this, as detailed in Section 5.5 (BCGF – Assets Model), would enable the Board to work with relevant CXOs to understand and agree on the priority assets, often referred to as crown-jewels. These can be processes, systems, data, or other assets that warrant protection from cybersecurity threats ahead of others in the organization. This enables a risk-based approach to investment in cybersecurity protection mechanisms. Should an organization already have such crown-jewels identified, then this model becomes less relevant, and potentially in this case, the Risk Appetite Statement Model could be of greater value. This model, as detailed in Section 5.6 (BCGF – Risk Appetite Statement Model) would enable the Board to discuss and agree on the extent to which cybersecurity impacts are tolerable and acceptable from a risk perspective. The expected practice implementation of the BCGF is shown in Figure 48 where the NIST Cybersecurity Framework (NIST, 2018) has been used to depict the application of the 7 foundational models in the appropriate stage of NIST. As can be seen here, the practice use of the BCGF is across all stages in the NIST Cybersecurity Framework.

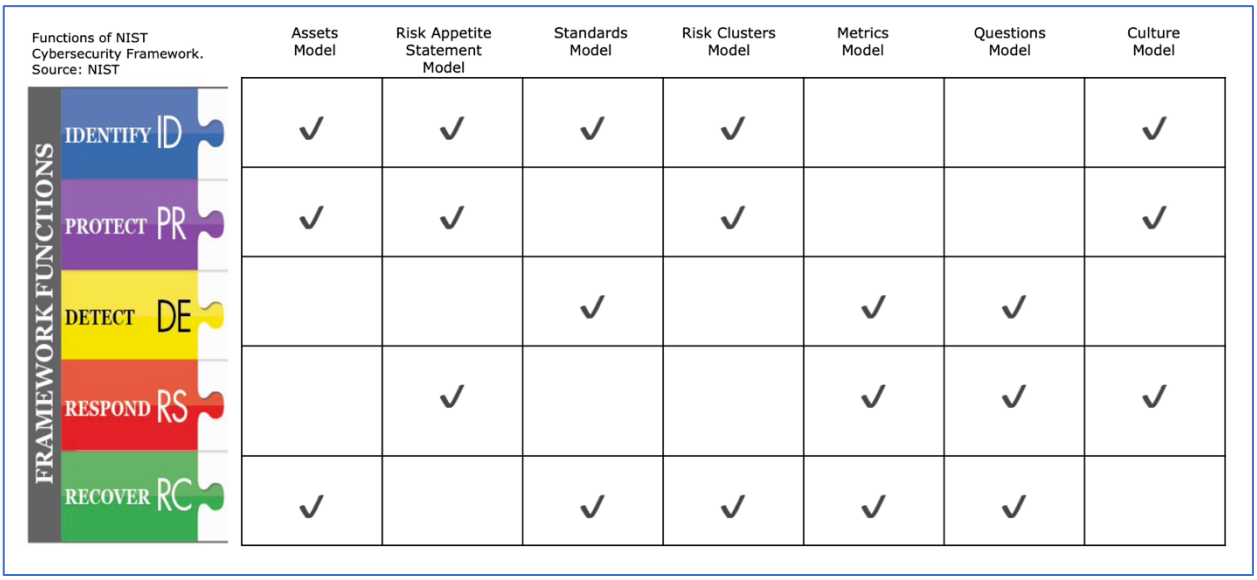

Figure 48: Relevance of BCGF models in NIST cybersecurity framework

7.4.3 Policy Implications

The long-term impact of a cybersecurity breach is detrimental to the brand and confidence levels in an organization, and good cybersecurity governance will assist in driving greater levels of trust in the organizations that serve the public, customers or other stakeholders (AICD, 2022a; Brown et al., 2017; Olyaei & Wheatman, 2022). Given the application of the BCGF assists NEDs to better govern cybersecurity posture, it is expected that its application and the inclusion of elements of this in policy, standards and professional learning material in organisations such as the AICD and ACSC, will only assist NEDs more broadly. Further, the application of the BCGF in specific scenarios can assist in implementing organizational policy and through this, assists in promoting the credentials of the organization amongst its stakeholders, such as clients and regulators. For example, through the Standards Models, as detailed in Section 5.7 (BCGF – Standards Model), understanding and agreeing on the specific standards to adopt,

can assist in setting the policy that informs the speed and manner in which a response to a cybersecurity incident is undertaken. Such notifications can be a differentiator for an organization that can be seen as being transparent and trustworthy in such situations, and be seen as accountable in a responsible way, as seen from in learnings from recent industry incidents at Medibank and Optus (APRA, 2023; OPTUS, 2023).

7.4.4 Generalisation For Industry

The positive reinforcement on the validity of the BCGF implies that it can be applied and used by NEDs in the course of their duties. The use is not limited to NEDs, given strong feedback also from CIOs/CISOs. CXOs who provide assurance to Boards. As such, CEOs, CIOs, CISOs and CROs may also benefit from an understanding of the BCGF and how they can better facilitate discussions and agreements with their respective Boards. The use of this framework will help stakeholders fulfil their cybersecurity governance accountabilities in the private or public sector. Based on the research in formulating the BCGF, it is expected that its application in relevant Boards will increase the confidence of NEDs individually and collectively. Through this, it is expected to bring about more awareness and transparency on cybersecurity risk, and over time, this should assist in creating greater levels of trust in the organization's digital platforms and services. The research problem is not limited to any one industry sector given the nature of cybersecurity. Whilst some sectors, such as financial services and government entities, face more sophisticated threats and attacks than others, the risks are not only limited to these sectors. Similarly, cybersecurity governance is a global issue, and threats, mitigations, and regulations often span geographic borders. The research included interviewees and validation experts with cross-industry and international expertise and therefore it is anticipated that the application of the BCGF will be easier across the broader industry. An example of this is the application of the Assets Model and Risk Appetite Statement Model, as detailed in Chapter 5 - Board Cybersecurity Governance Framework (BCGF), in sections 5.5 (BCGF – Assets Model) and 5.6 (BCGF – Risk Appetite Statement Model). In these models, the discussion on which assets (services, processes, systems, data, etc.) are critical to protect as a priority from a business perspective, has been described in a generalised manner, regardless of industry or geography. The process in the Assets Model, to agree on the assets, or crown-jewels to protect, is generic to enable applicability across industry sectors. Similarly, the Risk Appetite Statement Model factors in an approach that considers impacts from a cybersecurity incident that centre on general impacts to dimensions such as share price, revenue loss, data loss, resilience impacts and reputation. These dimensions can be changed in the model, and so for a government department, share price may not be relevant, but reputation carries more importance in the acceptable risk appetite. This generalised approach enables application to a broad set of organizations.

7.4.5 Cybersecurity Education and Awareness Implications

The BCGF and associated guidelines provide artefacts that can be directly leveraged in individual Board application, as already seen in Section v (List of Publications and Presentations) where Board presentations have already assisted NED stakeholders (and through this, helped to refine the BCGF during its formulation). Similarly, embedding the BCGF through alliances with organisations into regular Board education will assist in increasing the awareness of NEDs and establishing partnerships with NED professional bodies, such as AICD, will allow its value to further increase and also more importantly, will allow feedback to further improve this. The AICD and ACSC are driving a focus on Board Directors to improve their literacy in cybersecurity. Adopting and embedding the Risk Clusters Model, as detailed in Section 5.8 (BCGF – Risk Clusters Model) establishes an mechanism to demonstrate this in a proactive manner that has linkage to the risks and terminology directly relevant to the Board cybersecurity discussions for that risk horizon. This targeted approach to education and awareness can only help in improving skills and capability in cybersecurity at a Board level.

7.5 Risks and Limitations

The field of cybersecurity is an ever-changing, one as outlined previously in terms of the threats and sophistication of attacks, as well as the solutions available to mitigate these. Further, as outlined previously, regulation is also evolving in light of the risks, with more requirements being posed on Boards. This backdrop means that the BCGF will need to evolve as the environment around it changes. As such, the BCGF will require ongoing assessment on the extent to which it remains applicable to the NED and CXO roles. Additionally, as the understanding and capability in cybersecurity governance grows at a Board level, some models may become obsolete as such approaches may well migrate into the regular education and standards that are published by NED professional bodies such as the AICD or National Association of Corporate Directors (NACD). Further, over time, some of the models may become standard assumed knowledge and not require any specific guidance. This is akin to aspects of financial reporting, which are well embedded into standard Board reporting, with ratios, metrics and conventions established into accounting standards. One would hope frameworks such as the BCGF over the years evolve to become standardised ways of governing cybersecurity risk at a Board level.

Given these themes, a core limitation is one of currency, as the BCGF will require ongoing assessment for being practical in context of the operating environment. A mitigating step in such a limitation is the ability to adapt the framework to make it fit-for-purpose; it has been intentionally designed with this in mind for cross-industry use. The research stages included experts from cross-industry, government and the academic community to assist in making it practical for cross-industry. Further, the models are standalone and so Boards can choose to apply the models that make sense for their organization's maturity level and risk appetite.

Other risks such as research and researcher bias, and the challenges faced during the course of the research also present some limitations. Complimentary mechanisms were used to address and overcome these, and through this, minimise the possible omission of insights. For example, a key mitigant to research and researcher bias was to ensure that a set of highly experienced subject matter experts were engaged at the outset in participant interviews, and then in the expert evaluation workshop. Such deep and extensive experience, as detailed in Appendix 8.3, consisted of 34 years of cross-industry experience. However, access to these experts in terms of their availability was a challenge. Therefore, it was important to be flexible in accommodating the date, time and location constraints in their busy diaries. Flexibility, through virtual and physical location was critical. The size of the cohort for the interviews (15) and the expert evaluation workshop (20), could be considered a limitation, in spite of having highly experienced participants. This was addressed through statistical analysis of the expert evaluation survey, as detailed in Chapter 6 - Results and Evaluation. Further, at each stage of the research, insights were shared in fortnightly reviews with the supervisor. The annual Candidature Assessment also enabled a more independent and formal evaluation of the research by the co-supervisor, external supervisor, independent chair and subject matter advisor. In addition, where possible, as per the section on List of Publications and Presentations, draft insights of the emerging solution/BCGF were applied to specific Board meetings. Further, GT techniques enabled the deep synthesis of data, including classification, mapping and synthesis, to ensure the solution components were informed and backed up by rigorous research. A summary of the top risks and limitations, along with how the research has aimed to mitigate these, is presented in Table 53.

Risk / Limitation	Description	Consequences	Mitigants in Research
Risk	Cybersecurity governance is a changing field due to environmental factors.	BCGF may become outdated quickly.	Models have been designed at a logical level to enable adaption as change occurs.
Limitation	Maturity amongst NEDs may mean they need less assistance in specific areas of the BCGF scope.	Components of the model may cease to add value.	Models are all optional and a Board may choose the ones that relate to their level of maturity.
Limitation	Over time, models in BCGF become embedded in formal professional bodies and their training for NEDs.	This is a good thing, as the confidence to govern cybersecurity will improve.	The BCGF is extensible as the knowledge and know-how of NEDs improves. It will require a refresh when this happens.
Risk	The participants that informed the research had limited experience.	BCGF may not represent broader industry needs.	Interviewees and experts for evaluation workshop/survey were chosen from a breadth of industries and with an average of industry experience of 34 years.
Risk	Some parts of the BCGF may have been overlooked by participants.	BCGF review may have some omissions.	Complementary approaches used to mitigate the limitation of the reviews. This included, expert workshop, expert survey, GT techniques to synthesis one-on-one interviews to extract concerns, mapping of concerns to BCGF components, and statistical analysis to demonstrate validity.
Limitation	The BCGF and its models may not be perceived as technical in nature by the typical technical security SMEs.	Stakeholders who implement security (CISO, security/risk SME, etc) do not find the BCGF relevant to them.	The core aim and scope of the BCGF was to address unmet needs/research for NEDs. It has done that. SMEs should use the BCGF as a way to align their technical work to these practices and how their work supports the Board. Thus, the technical contents are beyond the scope of this work, which well covered in technical and operational frameworks such as NIST, COBIT etc.

Table 53: Top research risks and limitations with mitigants

7.6 Key Learnings

The research process provided many learnings in terms of aspects that were not known or understood fully at the start, which provided valuable insights into enriching the solution components themselves, or learnings that increased the skills and knowledge of the researcher. The journey for this research over 3.5 years was challenging, given the nature of an evolving topic, with a new industry focus and regulations emerging in the last 12 months following the initial literature review, and also prior academic literature not serving the NED audience to the same extent as the cybersecurity/risk SME. New grounds had to be established in this research given the intended target audience. Four broad categories of learnings were encountered, as detailed in Figure 49.

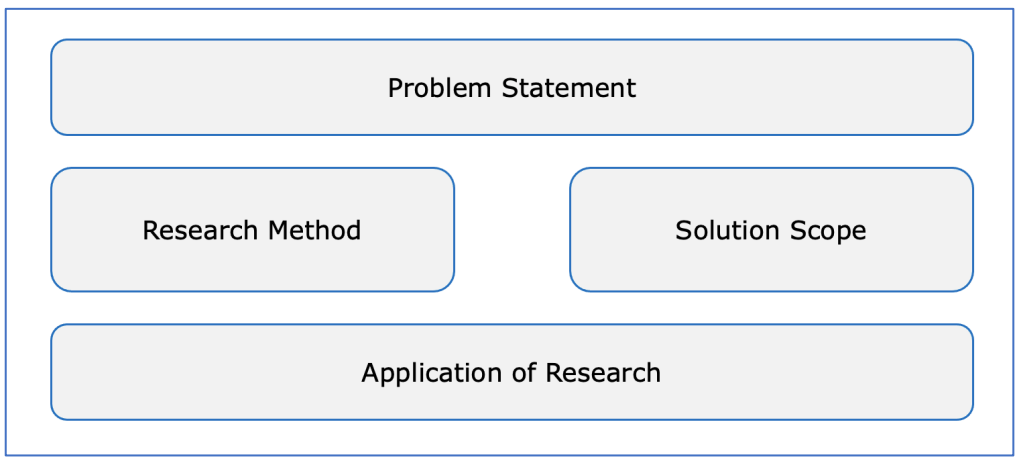

Figure 49: Categories of learning from research

Each category has a number of detailed learnings as expressed in Table 54.

Learning Category	Learning from the research process
Problem Statement	Cybersecurity is a shared concern amongst key stakeholders (NED, CIO, CISO) and is growing
Problem Statement	Severity of penalties exist on NEDs for poor cybersecurity governance
Problem Statement	Topic is central to multiple sectors beyond banking where traditionally this has been strong
Problem Statement	There was limited academic literature targeted at the NED audience
Problem Statement	Business literature is limited to high level principle based, with limited implementation guides
Problem Statement	Concerns expressed by stakeholders are a global problem as seen in actions from regulators, and expert review
Research Method	DSR provides a structured way to formulate and evaluate artefacts
Research Method	Grounded Theory techniques to analyse, code and synthesis results enhances DSR effectiveness
Research Method	Statistical analysis, such as chi-square and skewness, provide ways to enhance the validity of quantitative results
Research Method	Complimentary research techniques are necessary to thoroughly formulate and evaluate solution components
Research Method	Qualitative feedback from experts can be useful to enhance artefacts and is important to not ignore
Solution Scope	The pain points and aspirations distil down to a handful items that can be addressed
Solution Scope	The lifecycle approach to cybersecurity aligns well with senior business audiences
Solution Scope	The BCGF gained stronger positive support from experts than expected
Solution Scope	There was willingness from experts to contribute to solutions in interviews, workshop and survey
Solution Scope	An approach for just-in-time education was stronger than expected, versus lots of upfront training/education for NEDs
Application of Research	The importance of a business scenario approach to application of models to help NEDs
Application of Research	Ensuring flexibility in the use of models for various organizations, to make fit-for-purpose
Application of Research	Application of models will inevitably need to be adapted for specific organizational maturity and risk appetite
Application of Research	Importance of embedding the use of the framework into existing Board risk and strategy processes
Application of Research	Value of establishing a mechanism for improvement of the solution - by application or publication

Table 54: Learnings from research

7.7 Conclusion and Next Steps

The importance and need to manage cybersecurity risk has become increasingly more relevant as the dependency on online digital services has grown for many organizations. This is compounded by the fact that threats to the digital economy and overarching operational resilience have increased and continue to do so in sophistication and volume. In particular, governing for cybersecurity resilience is a critical imperative in this environment and regulators are imposing fines on individuals and organizations for poor cybersecurity. Board Directors and Senior Executives are apprehensive when it comes to governing the quality of their organization's cybersecurity. Cybersecurity for many senior business audiences is challenging, given the technical language in use and the ever-changing nature of the field as new intricate threats evolve in digital platforms. Whilst there has been a growth in awareness in recent years on the importance of cybersecurity at the Board level, there has been a lack of practical frameworks and models to guide such stakeholders.

This research has addressed the important research question of, "What framework should be developed to help non-technical audiences such as Board Directors and Senior Executives better govern cybersecurity?" This thesis proposes the Board Cybersecurity Governance Framework (BCGF) as a way to address this critical need. This framework consists of seven related models that guide and support Board level cybersecurity governance, covering assets, risk appetite statement, standards, risk clusters, metrics, questions and culture. Each model is accompanied by detail which covers the business scenario under which a model is used, the implementation guidelines, and the key stakeholders that may provide input and/or receive output from the model.

The proposed framework and underpinning models have been iteratively developed and evaluated by using the well-known design science research method. The initial version of the framework has been developed based on the literature review. This framework was further developed through design workshops and interviews with 15 Board Directors and related senior stakeholders. An expert evaluation workshop and an associated online survey with 20 experienced stakeholders were conducted to evaluate and refine the proposed framework. The evaluation results indicate that the proposed framework is appropriate for Board Directors and Senior Executives aiming to govern cybersecurity. Complementary design and evaluation techniques, supported by statistical analysis, were used to demonstrate validity of the research. Further, the sub-questions in the research have been addressed by specific components of the BCGF, as shown in Table 55.

Research sub-questions	**Research Deliverables**
What are the key *components* of this framework, that can be explicitly address the gaps seen for Board Directors and Senior Executives in a systematic and practical manner?	Within the BCGF, **7 foundational models** cover core areas for consideration in Board cybersecurity governance for Directors. These offer a practical and flexible way that can be applied in accordance with the maturity of an organization.
How should each of these components *be used in practice* by the Board of Directors as they interact with management to set the strategy, risk appetite and tone for cybersecurity?	Each BCGF Model in the BCGF has **detailed usage guidelines** that have been informed by research and expert input. These enable application in a range of areas, including strategic, risk and cultural aspects.
How can the framework allow Board Directors to maintain an *ongoing knowledge and awareness* of the cybersecurity risks and terminology that remains current and relevant to them?	Specific models in the BCGF, particularly the **Risk Clusters Model, enables a proactive manner for scoping the education curriculum** for Board Directors that is grounded on the currency and relevance of topics informed by risks across different horizons and sources.

Table 55: Deliverables for research sub-questions

While the proposed framework addresses the current research question in hand, it is important to acknowledge the dynamic nature of the cybersecurity field, which will warrant the continuous evolution and adaptation of the framework for different organizational contexts. These organizational contexts were observed in the expert evaluation workshop and expert evaluation survey, where some participants placed more importance on specific models in the BCGF than others. As per the qualitative feedback, this was due to differences in maturity and know-how in specific organizational contexts. Such considerations are important in the ongoing use of the framework and ensuring its application is fit-for-purpose. Furthermore, application of the BCGF in Boardroom scenarios will provide new insights on areas that may warrant further updates and extensions of the models. It is important improvements to the BCGF are informed from this practical application and use, as well as further academic research into the components of the framework.

The journey to help non-technical audiences better govern cybersecurity will be an ongoing one and will demand continued research and application to assist Board Directors and Senior Executives who inevitably have to govern and lead this ever-changing area.

8 Appendices

8.1 Synthesis of AICD Cyber Security Board Governance Principles

The concepts inherent in each of the five principles outlined in (AICD, 2022a) are synthesised and mapped using GT techniques into 7 overarching Cybersecurity Dimensions to aid the literature review.

Abstracted Cybersecurity Dimension	Principle #1	Principle #2	Principle #3	Principle #4	Principle #5
	Set clear roles and responsibilities	Develop, implement and evolve a comprehensive cyber strategy	Embed cyber security in existing risk management practices	Promote a culture of cyber resilience	Plan for a significant cyber security event
Leadership	define roles and responsibilities delegation board charter emerging trends governance of cyber security risk data assets customer services industry partners cyber insurance	cyber strategy identify data assets data governance framework identify digital assets documentation third-party risk protection mechnisms crown-jewels sensitive data / documents	cyber risk appetite balanced risk / opportunities	incentivise / reward testing - phishing penetration testing recognise and promote culture role play exercises conduct of staf upskilling	simulation execises communications approach reputational damage mitigations roles and responsibilities scenarios
Assurance	formalised board reporting ad-hoc informal reporting external expert external audit risk assessments	incident response plans understood vulnerabilities evaluation of risk controls	risk management framework regular assessments controls assessment three-lines of defence external review	incident response plan	incident response plan business continuity cyber reslience
Benchmarking	clear board reporting measurable metics trend data cyber risk maturity standards frameworks cyber resilience level	maturity assessment - independent cyber security frameworks	risk reporting	incentives KPIs	
Terminology	non-technical terminology demistify cyber security			training - management training - board upskilling diffentiated training	
Stakeholders	sub-committee subject matter experts management expertise	capability maturity - management capability maturity - board		communications collaboration	management board
Regulation	compliance technical compliance regulatory requirements	standards framework supplier performance / maturity		exceptions workarounds	

Table 56: Key concepts in (AICD, 2022) mapped to higher level dimensions

8.2 Ethics Approval

Saturday, December 9, 2023 at 16:05:09 Australian Eastern Daylight Time

Subject: Your ethics application has been approved as low risk - ETH22-7097
Date: Wednesday, 25 May 2022 at 11:09:57 pm Australian Eastern Standard Time
From: research.ethics@uts.edu.au
To: Asif Gill, Sarv Girn
CC: Research Ethics
Attachments: Ethics Application.pdf

Dear Applicant,

Re: ETH22-7097 - "Cybersecurity Governance"

Your local research office has reviewed your application and agreed that it now meets the requirements of the National Statement on Ethical Conduct in Human

Research (2007) and has been approved on that basis. You are therefore authorised to commence activities as outlined in your application, subject to any conditions detailed in this document.

You are reminded that this letter constitutes ethics approval only. This research project must also be undertaken in accordance with all UTS policies and guidelines including the Research Management Policy.

Your approval number is UTS HREC REF NO. ETH22-7097

Approval will be for a period of five (5) years from the date of this correspondence subject to the submission of annual progress reports.

The following standard conditions apply to your approval:

- Your approval number must be included in all participant material and advertisements. Any advertisements on Staff Connect without an approval number will be removed.
- The Principal Investigator will immediately report anything that might warrant review of ethical approval of the project to the Ethics Secretariat.
- The Principal Investigator will notify the Committee of any event that requires a modification to the protocol or other project documents, and submit any required amendments prior to implementation. Instructions on how to submit an amendment application can be found here.
- The Principal Investigator will promptly report adverse events to the Ethics Secretariat. An adverse event is any event (anticipated or otherwise) that has a negative impact on participants, researchers or the reputation of the University. Adverse events can also include privacy breaches, loss of data and damage to property.
- The Principal Investigator will report to the UTS HREC or UTS MREC annually and notify the Committee when the project is completed at all sites. The Principal Investigator will notify the Committee of any plan to extend the duration of the project past the approval period listed above.
- The Principal Investigator will obtain any additional approvals or authorisations as required (e.g. from other ethics committees, collaborating institutions, supporting organisations).
- The Principal Investigator will notify the Committee of his or her inability to continue as Principal Investigator including the name of and contact information for a replacement.

This research must be undertaken in compliance with the Australian Code for the Responsible Conduct of Research and National Statement on Ethical Conduct in Human Research.

You should consider this your official letter of approval.

If you have any queries about this approval, or require any amendments to your approval in future, please do not hesitate to contact your local research office or the Ethics Secretariat.

Ref: 12a

8.3 Experience of Interviewees

Participant	Current Role	Industry Experience (years)	Industry sectors worked in (only those >3years)	Industry ISIC Codes
P#1	CISO	25	Electricity, Financial Services, Consulting Services	D, J, K, N, S
P#2	CISO	19	Financial Services	J, K
P#3	CISO	42	Telecommunications, Consulting	J, R, S
P#4	CISO	40	Government (Public Service), Telecommunications, Utilities	B, D, F, O, S
P#5	CISO	31	Electricity, Financial Services, Consulting Services	D, J, K, N, S
P#6	CIO	33	Retail, Consulting, Industrial, Food, Consulting	C, G, I, J, S
P#7	CIO	21	Financial Services, R&D Technical,	M, K
P#8	CIO	35	Corporate Governance, Financial Services,	J, K, M, O, S
P#9	CIO	37	Government (Public Service), Buillding, Financial Services	F, L, K, O, Q, S
P#10	CIO	32	Government (Public Service)	D, E, I, J, P, Q, S
P#11	NED	33	Property, Financial Services, Building Services	F, J, K, L, O, S
P#12	NED	32	Insurance, Legal, Health	E, K, O, P, Q, S
P#13	NED	42	Technology, Financial Services, Transport, Education, Utilities	E, J, K, P,
P#14	NED	42	Financial Services, Telecommunications, Payments	J, K, M, H, S
P#15	NED	45	Financial Services, Property, Small Business	F, H, J, K, L, S
Average industry experience (years)		34		
Total industry experience (years)		509		

CISO - Chief Information Security Officer; CIO - Chief Information Officer; NED - Non Executive Director

ISIC - International Standard Industrial Classification (of all Economic Activities)

Table 57: Extent of industry experience (interviewees)

International Standard Industry Codes (ISIC)

Section	Description	# Participants
A	Agriculture, forestry and fishing	0
B	Mining and quarrying	1
C	Manufacturing	1
D	Electricity, gas, steam and air conditioning supply	4
E	Water supply; sewerage, waste management and remediation	3
F	Construction	4
G	Wholesale and retail trade; repair of motor vehicles and motorcycles	1
H	Transportation and storage	2
I	Accommodation and food service activities	2
J	Information and communication	11
K	Financial and insurance activities	11
L	Real estate activities	3
M	Professional, scientific and technical activities	3
N	Administrative and support service activities	2
O	Public administration and defence; compulsory social security	5
P	Education	3
Q	Human health and social work activities	3
R	Arts, entertainment and recreation	1
S	Other service activities	12
T	Activities of households as employers; undifferentiated goods- and services - producing activities of households for own use	0
U	Activities of extraterritorial organizations and bodies	0

Table 58: Coverage of industries by interviewees

8.4 Consent Forms

8.4.1 One on one Interview Consent Form

UTS UNIVERSITY OF TECHNOLOGY SYDNEY

PARTICIPANT INFORMATION SHEET: ONE ON ONE INTERVIEW

[ETH22-7097] - CYBERSECURITY GOVERNANCE FOR BOARDS

WHO IS CONDUCTING THIS RESEARCH?

My name is Sarv Girn and I am a Doctorate student at UTS and contactable on sarv.girn@uts.edu.au. My supervisor is Dr Asif Gill, who is the A/Professor & Director of the DigiSAS Lab at the UTS School of Computer Science in the Faculty of Engineering and IT. Dr Gill's email is asif.gill@uts.edu.au.

WHAT IS THE RESEARCH ABOUT?

The purpose of this research is to formulate a Cybersecurity Framework that can better support Senior Executives and Board Directors in the governance of Cybersecurity. The research will examine the use and value of specific artefacts, such as language/lexicon used in reports, foundational metrics to measure the health of cybersecurity, and the approach to tracking progress in the metrics through a form of security index.

WHY HAVE I BEEN INVITED?

You have been invited to participate in a one on one interview because of the industry experience you possess in either, presenting and reporting the health of cybersecurity to senior executives and board directors, or as a board director you have experience of receiving such updates from senior executives such as Chief Information Officers (CIO) or Chief Information Security Officers (CISO).

Your experience and exposure would have given you insights into what works and what doesn't work; including areas such as, the language used, the metrics that are important, and how over time improvement can be tracked in the metrics by board directors.

WHAT DOES MY PARTICIPATION INVOLVE?

If you decide to participate, I will invite you to a one on one meeting to inform the design of the draft framework artefacts.

By way of background, participants are required for one of two phases. All participants are chosen for their industry experience as recognised from their public professional profiles through various roles they have undertaken. As such, they are not representing (and will be requested to refrain from discussing) their employer or organisation; they would be providing an industry view point without reference to any organisation on cybersecurity governance artefacts as a CIO, CISO, Board Director, or industry/academic expert. If you are under any form of contract with an organisation you should confirm your have no restriction on providing such input.

The first phase involves one on one interviews with relevant CIOs, CISOs and Board Directors. It is expected that 12 participants in total will be interviewed in this phase, split equally across the three roles. The discussions from this phase across all the interviews will be further informed and enriched by relevant academic literature, theories and industry practices. This phase will formulate a final draft framework that will be evaluated in the second phase.

The second phase is an Expert Evaluation Workshop (EEW) by industry experts in the cybersecurity field, as related to reporting the status of this to senior executives and boards across the public and private sector. It is expected that 30 experts will participate in the EEW. Participants from the one on one interviews can optionally attend the workshop as well should they have an interest; this is however not mandatory.

The EEW will be presented with the final draft framework, and detailed feedback will be sought via an online survey in the workshop. This will enable questions and clarifications to be addressed in the session. Participants in the workshop will be industry leaders experienced in cybersecurity across aspects such as strategy, risk management, assurance reporting, board reporting and language, advisory, research, and systems architecture.

The time commitment for first phase participants (one on one interviews) will be 1 hour. The nature of the questions will be shared with participants one week before the meeting. Whilst no pre-work is required by participants, they may choose to spend up to 30min thinking through aspects of the questions. It is expected the meetings for the one on ones are virtual via MS Teams or Zoom. However, if a participant finds it more convenient to meet physically, then this would in a UTS Building (Building 11 or Building 2 at the Ultimo Campus), or the AICD offices in Sydney (18 Jamison Street). Should participants wish to suggest their own office location for the interviews, that would not be an issue. The interviews will not be recorded via audio or video; typed notes will be taken (with explicit permission sought in each meeting) with these held in a secure location within the UTS MS Office infrastructure.

The commitment for the second phase participants (EEW) will 1.5 hours and this will be virtual via Zoom to make attendance easier. The final draft framework of artefacts will be circulated two weeks prior to the workshop to participants. The agenda will include a 45min walkthrough of the framework and answering any clarifying questions, and then 45min for the online feedback survey. This will capture detailed feedback from the participants on artefacts of the framework. Furthermore, should some workshop participants wish to provide further feedback after the workshop, then they will be given this opportunity. The workshop will be recorded via the UTS Zoom which will store this within UTS systems; any typed notes will be taken with within the UTS MS Office infrastructure. The responses to the survey will be held securely within UTS systems environment.

ARE THERE ANY RISKS/INCONVENIENCE?

Yes, there are some risks/inconvenience but these would be minimal. The nature of the research is focussed on industry practices, and does not require correlation to specific organisations. If organisation names are mentioned inadvertently in the one on one interviews or the workshop, these will not be captured in the relevant notes and participants will be requested to refrain from mentioning organisations at the outset. The output from the research will not reference any company names or individual participant names.

For the workshops a date/time will need to be scheduled for the 30 participants. This may cause some inconvenience in having to shuffle diaries to accommodate dates/times that may be suitable for the majority of participants.

DO I HAVE TO TAKE PART IN THIS RESEARCH PROJECT?

Participation in this study is voluntary. It is completely up to you whether or not you decide to take part.
If you decide not to participate, or to withdraw from the study, it will not affect your relationship with the researchers or the University of Technology Sydney.

WHAT IF I WITHDRAW FROM THIS RESEARCH PROJECT?

If you wish to withdraw from the study once it has started, you can do so at any time without having to give a reason, by contacting Sarv Girn.

If you withdraw from the study, you can optionally also request any electronic notes that were taken from your contributions at the one on ones or from your contribution at the Expert Evaluation Workshop (whichever is relevant) are not used and are destroyed.

WHAT WILL HAPPEN TO INFORMATION ABOUT ME?

By signing the consent form you consent to the research team collecting and using personal information about you for the research project. Personal information will only consist of your name, email and mobile number. Information pertaining to the one on ones will be notes taken electronically in the meetings. Similarly notes from will be taken in the workshop electronically. No video or audio recordings will be made. The survey results and feedback will be held securely in UTS systems.

All this information will be treated confidentially and stored securely on UTS MS Office environment. Only the Researcher (Sarv Girn) and Supervisor (Dr Gill) will have access to this.

We would like to store your information for future use in research projects that are an extension of this research project. In all instances, your information will be treated as confidential and stored securely.

It is anticipated that the results of this research project will be published and/or presented in a variety of forums. In any publication and/or presentation, information will be provided in such a way that you cannot be identified, except with your permission. If that permission was granted then this would be to only mention that you were a participant in this research.

In accordance with relevant Australian and/or NSW Privacy laws, you have the right to request access to the information about you that is collected and stored by the research team. You also have the right to request that any information with which you disagree be corrected. Please inform the research team member named at the end of this document if you would like to access your information.

The results of this research may also be shared through open access (public) scientific databases, including internet databases. This will enable other researchers to use the data to investigate other important research questions. Results shared in this way will always be de-identified by removing all personal information (e.g. name, address, date of birth etc.).

WHAT IF I HAVE ANY QUERIES OR CONCERNS?

If you have queries or concerns about the research that you think I or my supervisor can help you with, please feel free to contact me on sarv.girn@uts.edu.au or my supervisor Dr Asif Gill on asif.gill@uts.edu.au.

You will be given a copy of this form to keep.

NOTE:
This study has been approved in line with the University of Technology Sydney Human Research Ethics Committee [UTS HREC] guidelines. If you have any concerns or complaints about any aspect of the conduct of this research that you wish to raise independently of the research team, please contact the Ethics Secretariat on ph.: +61 2 9514 2478 or email: Research.Ethics@uts.edu.au], and quote the UTS HREC reference number. Any matter raised will be treated confidentially, investigated and you will be informed of the outcome.

CONSENT FORM – ONE ON ONE INTERVIEW

[ETH22-7097] - CYBERSECURITY GOVERNANCE FOR BOARDS

I _____ *[participant's name]* agree to participate in the research project (one on one interview and optionally the Expert Evaluation Workshop) being conducted by Sarv Girn, sarv.girn@uts.edu.au, mobile [redacted].

I have read the Participant Information Sheet or someone has read it to me in a language that I understand.

I understand the purposes, procedures and risks of the research as described in the Participant Information Sheet.

I have had an opportunity to ask questions and I am satisfied with the answers I have received.

I freely agree to participate in this research project as described and understand that I am free to withdraw at any time without affecting my relationship with the researchers or the University of Technology Sydney.

I understand I am aware of no contractual restriction that may prohibit me from contributing towards this research.

I understand that I will be given a signed copy of this document to keep.

I am aware that I can contact Sarv Girn or the Supervisor (Dr Asif Gill, asif.gill@uts.edu.au) if I have any concerns about the research.

_____ ____/____/____

Name and Signature [participant] Date

Production Note:
Signature removed prior to publication.

Sarv Girn

_____ ____/____/____

Name and Signature [researcher] Date

8.4.2 Workshop Consent Form

UTS UNIVERSITY OF TECHNOLOGY SYDNEY

PARTICIPANT INFORMATION SHEET & CONSENT FORM

EXPERT EVALUATION WORKSHOP

[ETH22-7097] - CYBERSECURITY GOVERNANCE FOR BOARDS

WHO IS CONDUCTING THIS RESEARCH?

Sarv Girn, a Doctorate student at UTS is conducting this research. The supervisor for this is Dr Asif Gill, Head of Discipline, Software Engineering at the School of Computer Science in the Faculty of Engineering and IT.

WHAT IS THE RESEARCH ABOUT?

The purpose of this research is to formulate a Board Cybersecurity Framework that can better support Senior Executives and Board Directors in the governance of Cybersecurity.

WHY HAVE I BEEN INVITED?

You have been invited to participate in an Expert Evaluation Workshop (EEW) because of the industry experience you possess. This may be as an advisor, a senior executive that reports the health of cybersecurity to Board Directors, or as a Board Director that receives updates from senior executives such as Chief Information Officers (CIO) and/or Chief Information Security Officers (CISO). Your experience and exposure would have given you insights into what works, what doesn't work, and specifically where board directors may need more help to govern cybersecurity risk.

WHAT DOES MY PARTICIPATION INVOLVE?

The workshop of approximately 30 attendees will be virtual and no longer than 1.5 hours. A presentation of the Board Cybersecurity Governance Framework (BCGF) will be conducted first, followed by some questions and answers, and finally an online survey to seek feedback.

Participants in the workshop will be industry leaders experienced in cybersecurity across aspects such as strategy, risk management, assurance reporting, board reporting, advisory, and research.

The workshop will be recorded, and the responses to the survey will be held securely within UTS systems environment.

ARE THERE ANY RISKS IN PARTICIPATION?

There are negligible risks due to the nature of the research, which is focussed on industry practices, and does not require correlation to specific organisations. The output from the research will not reference any company names or individual participant names.

DO I HAVE TO TAKE PART IN THIS WORKSHOP?

Participation in this study is voluntary. It is completely up to you whether or not you decide to take part. If you decide not to participate, or to withdraw from the study, it will not affect your relationship with the researcher or the University of Technology Sydney. You can decline the invitation should you wish to withdraw.

UTS UNIVERSITY OF TECHNOLOGY SYDNEY

WHAT WILL HAPPEN TO INFORMATION ABOUT ME?

By signing the consent form you consent to the research team collecting and using personal information about you for the research project. Personal information will only consist of your name and email address, and not be correlated to your survey responses (which remain anonymous).

All this information will be treated confidentially and stored securely on UTS MS Office environment. Only the Researcher (Sarv Girn) and Supervisor (Dr Gill) will have access to this.

We would like to store your information for future use in research projects that are an extension of this research project. In all instances, your information will be treated as confidential and stored securely.

It is anticipated that the results of this research project will be published and/or presented in a variety of forums. In any publication and/or presentation, information will be provided in such a way that you cannot be identified, except with your permission. If that permission was granted then this would be to only mention that you were a participant in this research.

In accordance with relevant Australian and/or NSW Privacy laws, you have the right to request access to the information about you that is collected and stored by the research team. You also have the right to request that any information with which you disagree be corrected. Please inform the research team member named at the end of this document if you would like to access your information.

The results of this research may also be shared through open access (public) scientific databases, including internet databases. This will enable other researchers to use the data to investigate other important research questions. Results shared in this way will always be de-identified by removing all personal information (e.g. name, address, date of birth etc.).

WHAT IF I HAVE ANY QUERIES OR CONCERNS?

If you have queries or concerns about the research that you think I or my supervisor can help you with, please feel free to contact me on sarv.girn@uts.edu.au or my supervisor Dr Asif Gill on asif.gill@uts.edu.au.

NOTE:
This study has been approved in line with the University of Technology Sydney Human Research Ethics Committee [UTS HREC] guidelines. If you have any concerns or complaints about any aspect of the conduct of this research that you wish to raise independently of the research team, please contact the Ethics Secretariat on ph.: +61 2 9514 2478 or email: Research.Ethics@uts.edu.au], and quote the UTS HREC reference number found at the top of this page. Any matter raised will be treated confidentially, investigated and you will be informed of the outcome.

CONSENT FORM – EXPERT EVALUATION WORKSHOP

[ETH22-7097] - CYBERSECURITY GOVERNANCE FOR BOARDS

I _____ *[participant's name]* agree to participate in the research project (Expert Evaluation Workshop) being conducted by Sarv Girn, sarv.girn@uts.edu.au, mobile [redacted]

I have read the Participant Information Sheet or someone has read it to me in a language that I understand.

I understand the purposes, procedures and risks of the research as described in the Participant Information Sheet.

I have had an opportunity to ask questions and I am satisfied with the answers I have received.

I freely agree to participate in this research project as described and understand that I am free to withdraw at any time without affecting my relationship with the researchers or the University of Technology Sydney.

I understand I am aware of no contractual restriction that may prohibit me from contributing towards this research.

I understand that I will be given a signed copy of this document to keep.

I am aware that I can contact Sarv Girn or the Supervisor (Dr Asif Gill, asif.gill@uts.edu.au) if I have any concerns about the research.

_____ ____/____/____

Name and Signature [participant] Date

Production Note:
Signature removed prior to publication.

Sarv Girn 3rd July 2023

_____

Name and Signature [researcher] Date

8.5 Interview Structure & Questions

8.5.1 One on one DIRECTOR Questions

UTS UNIVERSITY OF TECHNOLOGY SYDNEY

PARTICIPANT INFORMATION SHEET: ONE ON ONE QUESTIONS FOR DIRECTORS

[ETH22-7097] - CYBERSECURITY GOVERNANCE FOR BOARDS

PAIN POINTS & ASPIRATIONS

1. What challenges or pain points to you experience when you receive cybersecurity reports as a Board Director, or Member of a Risk Committee?
2. Do you have any ideas or aspirations on how these pain points can be addressed in a pragmatic and practical way?

LANGUAGE

3. How have you managed to understand the complex cybersecurity technical terminology that some reports or executives use?
4. Have you undertaken any specific training or used other mechanisms to assist in this regard?

METRICS

5. What type of metrics have typically been useful when you are presented with cybersecurity reports?
6. How have you been shown improvements in a fact-based manner in the cybersecurity risk profile (when improvement is required)?

OTHER

7. Are there any other approaches you would suggest to make cybersecurity reporting more effective and meaningful to Board Directors?

8.5.2 One on one CIO CISO Questions

UTS UNIVERSITY OF TECHNOLOGY SYDNEY

PARTICIPANT INFORMATION SHEET: ONE ON ONE QUESTIONS FOR CIO AND CISO

[ETH22-7097] - CYBERSECURITY GOVERNANCE FOR BOARDS

PAIN POINTS & ASPIRATIONS

1. What challenges or pain points do you experience when you provide cybersecurity reports to Boards?
2. Do you have any ideas or aspirations on how these pain points can be addressed in a pragmatic and practical way?

LANGUAGE

3. How have you managed to convey complex cybersecurity technical terminology to Boards in a way that they can understand?
4. Have your Board Directors expressed interest in specific training or other mechanisms to assist them?

METRICS

5. In your reporting to the Board, what is the nature of the key metrics you provide in cybersecurity reporting?
6. How do you show changes in this risk profile in terms of trends or change in maturity?

OTHER

7. Are there any other approaches you have used to make cybersecurity reporting more effective and meaningful to Board Directors?

8.6 Expert Evaluation Workshop

8.6.1 Context and Problem Statement

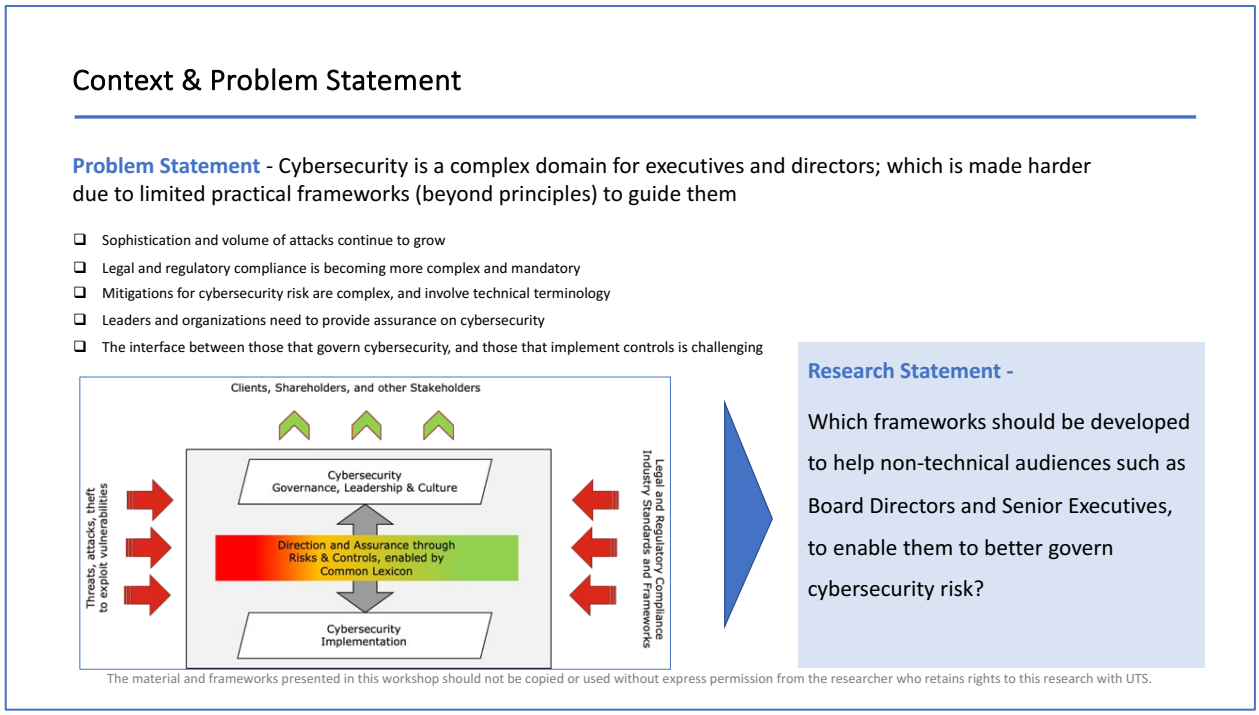

Figure 50: EEW: context and problem statement

8.6.2 Approach and Scope of Workshop

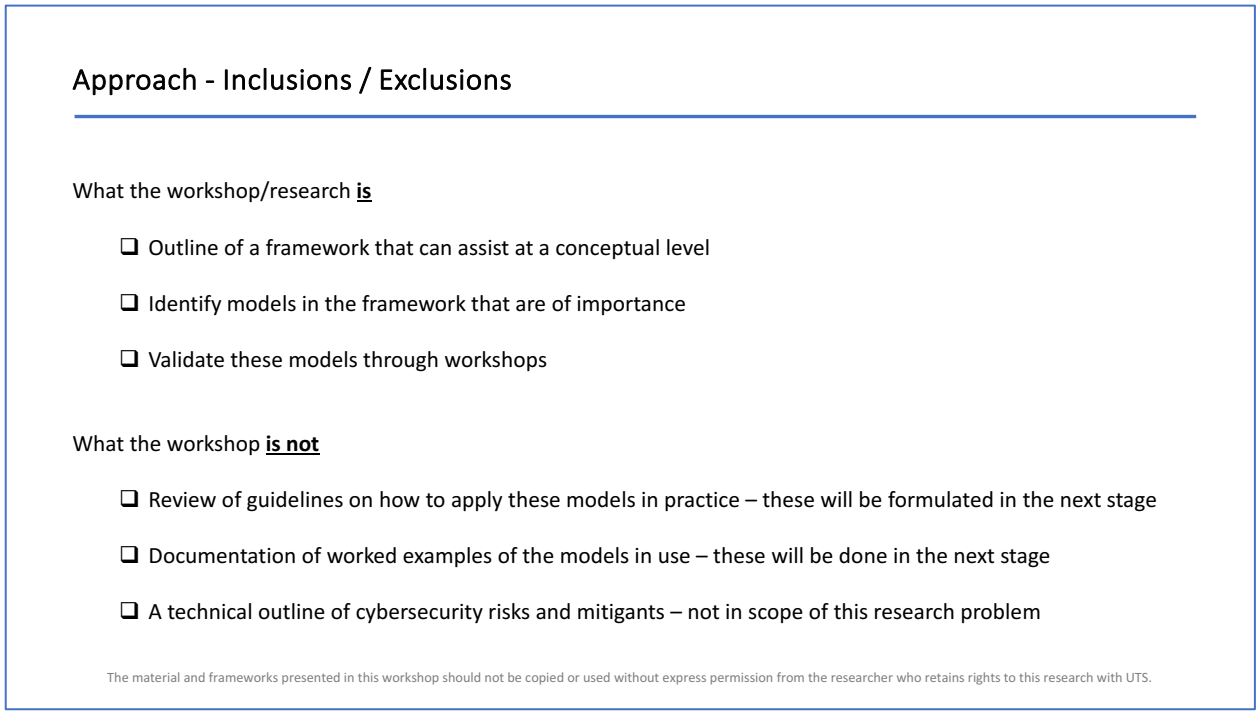

Figure 51: EEW: approach and scope of workshop

8.7 Expert Evaluation Survey Structure

8.7.1 Consent Request

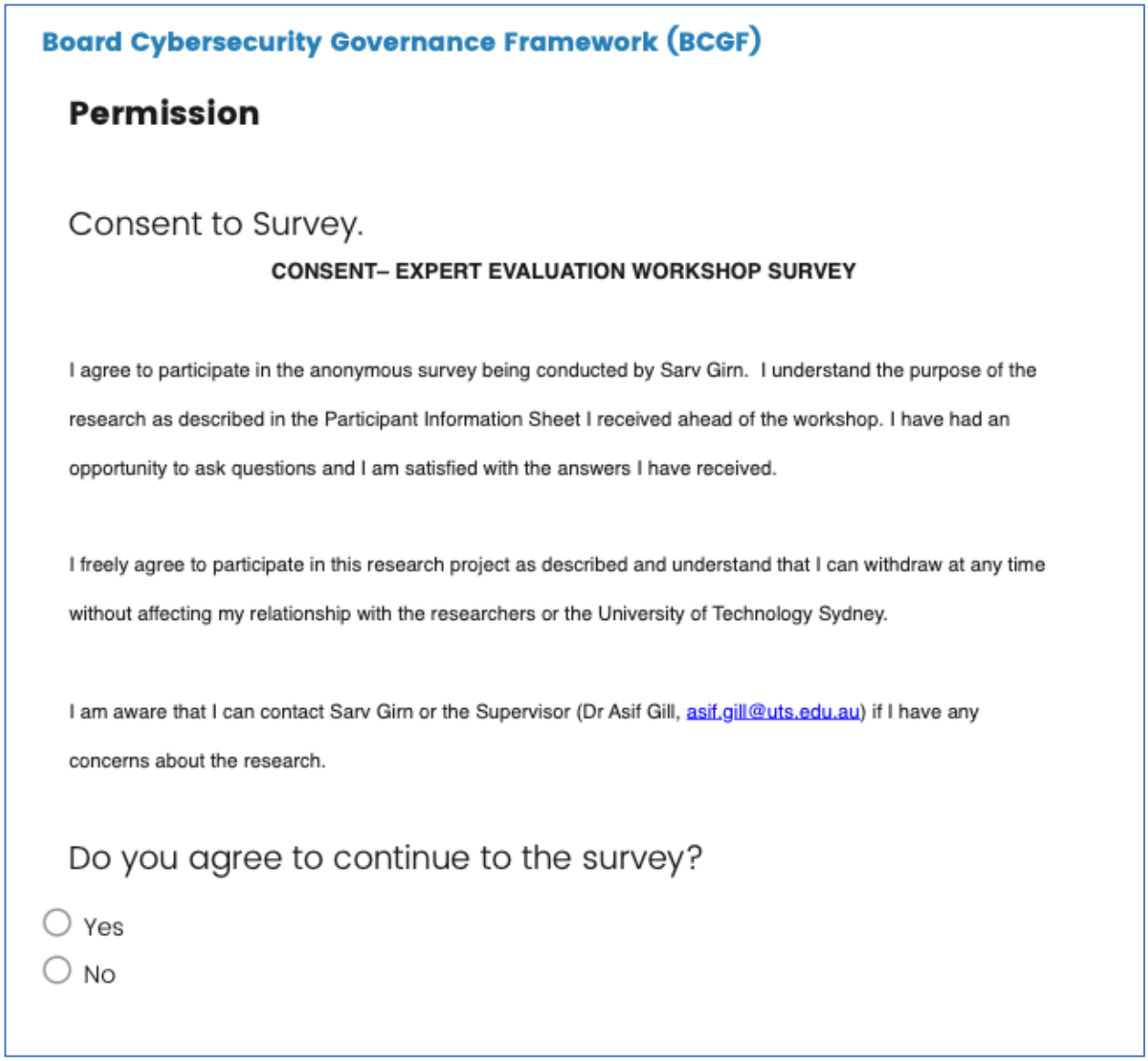

Figure 52: Expert evaluation survey consent

8.7.2 Questions

Responses captured on a 5-point scale (1 – Strongly Agree, 2 – Agree, 3 – Neutral, 4 – Disagree, 5 – Strongly Disagree).

Category		Question #	Question
Completeness	The extent to which is the BCGF (#1) is complete for Board Directors when they govern cybersecurity		
		1	The BCGF (#1) covers the important elements a Board Director should focus on when governing cybersecurity
		2	The lifecycle approach to cybersecurity governance is relevant to Board Directors given their role across strategic and operational matters
		3	Assurance (Management and Independent sources) is very relevant across all parts of the BCGF and should be examined separately and explicitly
Importance	The extent to which would the seven models of the BCGF are important (applicable) to a Board Director		
		4	Identifying the Assets to protect is an important aspect in the BCGF (Model #2)
		5	Establishing a clear cybersecurity risk appetite statement is important in the BCGF (Model #3)
		6	Agreeing a set of standards to comply with is important in the BCGF (Model #4)
		7	Establishing and maintaining risk clusters is important in the BCGF (Model #5)
		8	Embedding a portfolio of metrics is important in the BCGF (Model #6)
		9	Guidance to frame cybersecurity questions is important in the BCGF (Model #7)
		10	Understanding and guiding the cybersecurity culture is important in the BCGF (Model #8)
Relevance	The extent to which the seven models of the BCGF are relevant (valuable) tools for board directors when they govern cybersecurity risk in the course of their role		
		11	Identifying and understanding the Assets to protect is relevant for a Board Director
		12	Establishing cybersecurity risk specifically into the Risk Appetite Statement is relevant for a Board Director
		13	Establishing a baseline set of cybersecurity standards to govern against is relevant for a Board Director
		14	Reviewing and endorsing themes (risk clusters) that informs cybersecurity risk agenda is relevant for a Board Director
		15	Guiding a portfolio of metrics to inform the cybersecurity risk posture is relevant for a Board Director
		16	Guidance on how to structure cybersecurity questions that span multiple dimensions are relevant for a Board Director
		17	Having a clear idea of the desired cybersecurity culture in the organisation is very relevant for a Board Director
Practicality	The extent to which the elements of the BCGF and it seven models are a practical starting point for adaption and adoption into relevant Boards		
		18	The BCGF provides directors with a sound set of models to apply when governing cybersecurity
		19	The BCGF is easy to understand
		20	The BCGF is a practical toolkit that can be used to better govern cybersecurity as a board director
		21	The inclusion of a range of models in the BCGF enables a fit-for-purpose approach in its application
Improvements	The capture of further improvements you would suggest for Board Directors		
		22	Which elements of the BCGF would you remove ?
		23	What other elements would you add to the BCGF ?
		24	What other improvements would you like to add to the BCGF ?

Table 59: Expert evaluation survey question

9 References

ACSC. (2021). *Australian Cyber Security Centre (ACSC)*. https://www.cyber.gov.au/

ACSC. (2022). *ACSC Annual Cyber Threat Report, July 2021 to June 2022*. Australian CyberSecurity Centre (ACSC). https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022

AEMO. (2019, 9 Dec 2020). *Australian Energy Sector Cyber Security Framework (AESCSF)*. Australian Energy Market Operator (AEMO). https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources

AEMO. (2023). *AESCSF framework*. https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources

AICD. (2022a, October 2022). *Cyber Security Governance Principles*. https://www.aicd.com.au/content/dam/aicd/pdf/tools-resources/director-tools/board/cyber-security-governance-principles-web3.pdf

AICD. (2022b). *Cybersecurity - Are you taking the necessary steps and measures to reduce your exposure*. Australian Institute of Company Directors (AICD). https://aicd.companydirectors.com.au/global/taxonomydetail?tax=Cybersecurity

AICD. (2024a). *Corporate Governance Framework*. https://www.aicd.com.au/about-aicd/aicd-membership/director-professional-development/corporate-governance-framework.html

AICD. (2024b, 28-Feb-2024). *Governing Through a Cyber Crisis - Cyber Incident Response and Recovery for Australian Directors*. AICD. https://www.aicd.com.au/risk-management/framework/cyber-security/governing-through-a-cyber-crisis-cyber-incident-response-and-recovery-for-australian-directors.html

AICPA. (2018). *SOC for Cybersecurity: A Backgrounder*. https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/soc-for-cybersecurity- backgrounder.pdf

AICPA. (2022). Service Organization Control Type 2 (SOC2).

Albawaba. (2017). United States : IBM & Ponemon Institute: Cost of a Data Breach Dropped 10 Percent Globally in 2017 Study. *MENA Report*.

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond Choo, K.-K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security, 119*, 102754. https://doi.org/10.1016/j.cose.2022.102754

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review [Article]. *Computers and Security, 99*, Article 102030. 10.1016/j.cose.2020.102030

Allen, J. (2005). *Governing for Enterprise Security*. Carnegie Mellon Software Engineering Institute. https://apps.dtic.mil/sti/pdfs/ADA441250.pdf

Anderson, C., Baskerville, R. L., & Kaul, M. (2017). Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information. *Journal of Management Information Systems, 34*(4), 1082-1112. 10.1080/07421222.2017.1394063

APRA. (2010). *CPS 231 Outsourcing*.

APRA. (2019). *CPS 234 Information Security*. https://www.legislation.gov.au/Details/F2018L01745

APRA. (2023). *APRA takes action against Medibank Private in relation to cyber incident*. APRA. https://www.apra.gov.au/news-and-publications/apra-takes-action-against-medibank-private-relation-to-cyber-incident

ASD. (2020). *Essential Eight*. https://www.cyber.gov.au/acsc/view-all-content/essential-eight

ASD. (2023). Information Security Manual (ISM).

ASIC. (2015). *Cyber resilience: Health check* (Report 429). https://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf

ASIC. (2019). *Cyber resilience of firms in Australia's financial markets: 2018–19*. ASIC. https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-651-cyber-resilience-of-firms-in-australia-s-financial-markets-2018-19/

ASIC. (2020, 21 Aug 2020). *ASIC commences proceedings against RI Advice Group Pty Ltd for alleged failure to have adequate cyber security systems*. ASIC. https://asic.gov.au/about-asic/news-centre/find-a-media-release/2020-releases/20-191mr-asic-commences-proceedings-against-ri-advice-group-pty-ltd-for-alleged-failure-to-have-adequate-cyber-security-systems/

ASIC. (2022). *Cyber resilience in Australia's financial markets*. ASIC. https://asic.gov.au/regulatory-resources/markets/resources/markets-articles-by-asic/cyber-resilience-in-australia-s-financial-markets/

ASX/ASIC. (2017). *ASX 100 Cyber Health Check Report*. ASX/ASIC. https://www.asx.com.au/documents/investor-relations/ASX-100-Cyber-Health-Check-Report.pdf

AustCyber. (2021). *Australian Cyber Security Growth Network*. https://www.austcyber.com/about-us

Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: context and shared concepts. *Journal of cyber policy, 3*(2), 258-283. 10.1080/23738871.2018.1520271

Bailey, T., Banerjee, S., Feeney, C., & Hogsett, H. (2020). *Cybersecurity: Emerging challenges and solutions for the boards of financial- services companies*. McKinsey. McKinsey.

Bailey, T., Kaplan, J., & Rezek, C. (2014). *Why senior leaders are the front line against cyberattacks*. McKinsey. McKinsey.

Banker, R. D., & Feng, C. (2019). The Impact of Information Security Breach Incidents on CIO Turnover [Article]. *Journal of Information Systems, 33*(3), 309-329. 10.2308/isys-52532

Bassey, M. (1999). *Case study research in educational settings*. McGraw-Hill Education (UK).

Baxter, R. J., Holderness Jr, D. K., & Wood, D. A. (2016). Applying Basic Gamification Techniques to IT Compliance Training: Evidence from the Lab and Field [Article]. *Journal of Information Systems, 30*(3), 119-133. 10.2308/isys-51341

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems [Article]. *MIS Quarterly, 11*(3), 369-386. 10.2307/248684

Benbasat, I., & Zmud, R. W. (1999). Empirical Research in Information Systems: The Practice of Relevance. *MIS Quarterly, 23*(1), 3-16. 10.2307/249403

Boehm, J., Curcio, N., Merrath, P., Shenton, L., & Stähle, T. (2019). *The risk-based approach to cybersecurity*. McKinsey. McKinsey.

Brown, J. O., Marcum, J. A., & Stuebs Jr, M. T. (2017). Professional Virtue Reinforcements: A Necessary Complement to Technological and Policy Reforms [Article]. *Journal of Information Systems, 31*(2), 5-23. 10.2308/isys-51664

Bruin, R. D., & Solms, S. H. v. (2016, 11-13 May 2016). Cybersecurity Governance: How can we measure it? 2016 IST-Africa Week Conference.

Buchanan, S., Proctor, P., & Hayes, B. (2022). *Measure the Real Cost of Cybersecurity Protection*. Gartner.

Butler, S. (2017). *Macquarie dictionary* (Seventh edition. ed.). Macquarie Dictionary Publishers.

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2021). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis*. 10.1111/risa.13687

Cambridge English Dictionary. https://dictionary.cambridge.org/dictionary/english/cybersecurity

Canongia, C., & Mandarino, R. (2012). Cybersecurity: The New Challenge of the Information Society (Vol. 1, pp. 165-184).

CAQ. (2018). *Cybersecurity Risk Management Oversight*. thecaq.org

Carcary, M., Renaud, K., McLaughlin, S., & Brien, C. O. (2016). A Framework for Information Security Governance and Management. *IT Professional, 18*(2), 22-30. 10.1109/MITP.2016.27

Cebula, J. J., Popeck, M. E., & Young, L. R. (2014). A Taxonomy of Operational Cyber Security Risks Version 2.

Cheong, A., Yoon, K., Cho, S., & No, W. G. (2021). Classifying the Contents of Cybersecurity Risk Disclosure through Textual Analysis and Factor Analysis [Article]. *Journal of Information Systems, 35*(2), 179-194. 10.2308/ISYS-2020-031

CII. (2016). *Prioritizing Cybersecurity*. Council of Institutional Investors.

CIS. (2021). *CIS Critical Security Controls V8*. https://www.cisecurity.org/controls

CISA. (2019, 14 Nov 2019). *What is cybersecurity?* Cybersecurity & Infrastructure Security Agency, USA. https://us-cert.cisa.gov/ncas/tips/ST04-001

CISCO. (2021). *What is cybersecurity?* CISCO. https://www.cisco.com/c/en_au/products/security/what-is-cybersecurity.html

Clinton, L., Higgins, J., & van der Oord, F. (2020). *Cybersecurity Risk Management Oversight*. National Association of Corporate Directors and the Internet Security Alliance. https://www.nacdonline.org/applications/secure/?FileID=302181

Coden, M., Reeves, M., Pearlson, K., Madnick, S., & Berriman, C. (2023). An Action Plan for Cyber Resilience. *MIT Sloan Management Review, 64*(2), 1-6.

Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry, 114*, 103165. https://doi.org/10.1016/j.compind.2019.103165

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review, 4*(10).

Cram, W. A., & D'Arcy, J. (2023). 'What a waste of time': An examination of cybersecurity legitimacy [Article]. *Information Systems Journal, 33*(6), 1396-1422. 10.1111/isj.12460

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2021). When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal, 31*(4), 521-549. https://doi.org/10.1111/isj.12319

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems, 26*(6), 605-641. 10.1057/s41303-017-0059-9

CyBOK. (2021). *The Cyber Security Body of Knowledge*. National Cyber Security Centre (UK). https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

D'Arcy, J., & Basoglu, K. A. (2022). The Influences of Public and Institutional Pressure on Firms' Cybersecurity Disclosures [Article]. *Journal of the Association for Information Systems, 23*(3), 779-805. 10.17705/1jais.00740

Dedeke, A., & Masterson, K. (2019). Contrasting cybersecurity implementation frameworks (CIF) from three countries. *Information & Computer Security, 27*(3), 373-392. 10.1108/ICS-10-2018-0122

Deng, Q., & Ji, S. (2018). A review of design science research in information systems: concept, process, outcome, and evaluation. *Pacific Asia journal of the association for information systems, 10*(1), 2.

Dhillon, G., Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. *The Journal of Strategic Information Systems, 30*(4), 101693. https://doi.org/10.1016/j.jsis.2021.101693

Donalds, C., & Osei-Bryson, K.-M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management, 51*, 102056. https://doi.org/10.1016/j.ijinfomgt.2019.102056

Donaldson, S., Siegel, S., Williams, C. K., & Aslam, A. (2015). *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats* (1st edition ed.). Apress L. P. 10.1007/978-1-4302-6083-7

Doynikova, E., Fedorchenko, A., & Kotenko, I. (2019, 2019). Ontology of Metrics for Cyber Security Assessment.*ARES '19* ACM International Conference Proceeding Series.

Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. *Computers & Security, 132*, 103372. https://doi.org/10.1016/j.cose.2023.103372

Evans, N., & Price, J. (2020). Development of a holistic model for the management of an enterprise's information assets. *International Journal of Information Management, 54*, 102193. https://doi.org/10.1016/j.ijinfomgt.2020.102193
Fernandez, W. D., Lehmann, H., & Underwood, A. (2002). Rigor and relevance in studies of IS innovation: A grounded theory methodology approach.
FISMA. (2014). Federal Information Security Modernization Act. In C. I. S. Agency (Ed.). CISA. https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act
Flyvbjerg, B. (2006). Five Misunderstandings About Case-Study Research. *Qualitative Inquiry, 12*(2), 219-245. 10.1177/1077800405284363
Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2019). How Disclosing a Prior Cyberattack Influences the Efficacy of Cybersecurity Risk Management Reporting and Independent Assurance [Article]. *Journal of Information Systems, 33*(3), 183-200. 10.2308/isys-52374
Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security, 2017*(2), 5-10. https://doi.org/10.1016/S1361-3723(17)30013-1
Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security, 121*, 102840. https://doi.org/10.1016/j.cose.2022.102840
GCHQ. (2023). *Cyber Essentials: Requirements for IT infrastructure v3.1* https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-April-2023.pdf
Gielens, K., & Steenkamp, J.-B. E. M. (2019). Branding in the era of digital (dis)intermediation. *International Journal of Research in Marketing, 36*(3), 367-384. https://doi.org/10.1016/j.ijresmar.2019.01.005
Gill, A. Q., & Chew, E. (2019). Configuration information system architecture: Insights from applied action design research. *Information & management, 56*(4), 507-525. 10.1016/j.im.2018.09.011
Girn, S. (2022). A Data Driven Approach to Board Cybersecurity Governance. Pacific Asia Conference on Information Systems 2022.
Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory : strategies for qualitative research*. Aldine Pub. Co.
Gordon, S. (2023a). *Medibank Data Breach Class Action*. Slater and Gordon. https://www.slatergordon.com.au/class-actions/current-class-actions/medibank
Gordon, S. (2023b). *Optus Data Breach Class Action*. Slater and Gordon. https://www.slatergordon.com.au/class-actions/current-class-actions/optus-data-breach
Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly, 37*(2), 337-355. 10.25300/MISQ/2013/37.2.01
Groysberg, B., & Cheng, J. Y.-J. (2017). Directors aren't dealing with cyberthreats [Article]. *Harvard Business Review HBR, 95*(3), 36-36.
Gummesson, E. (2000). *Qualitative methods in management research*. Sage.
Guthrie, C., Fosso-Wamba, S., & Arnaud, J. B. (2021). Online consumer resilience during a pandemic: An exploratory study of e-commerce behavior before, during and after a COVID-19 lockdown. *Journal of Retailing and Consumer Services, 61*, 102570. https://doi.org/10.1016/j.jretconser.2021.102570
Haislip, J., Lim, J.-H., & Pinsker, R. (2021). The Impact of Executives' IT Expertise on Reported Data Security Breaches. *Information Systems Research, 32*(2), 318-334. 10.1287/isre.2020.0986
Harmer, G. (2013). *Governance of enterprise IT based on COBIT 5 : a management guide* (1st edition ed.). IT Governance Publishing.
Hevner, A., & Chatterjee, S. (2010). Design science research in information systems. *Design research in information systems, 22*, 9-22.
Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science In Information Sydtems Research. *MIS Quarterly, 28*(1), 75-105.

Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The Relationship between Board-Level Technology Committees and Reported Security Breaches [Article]. *Journal of Information Systems, 30*(3), 79-98. 10.2308/isys-51402

Iden, J., & Eikebrokk, T. R. (2013). Implementing IT Service Management: A systematic literature review. *International Journal of Information Management, 33*(3), 512-523. https://doi.org/10.1016/j.ijinfomgt.2013.01.004

IEEE Xplore. (2000). *IEEExplore*. IEEE.

ISACA. (2022). *Certified Information Security Manager (CISM)*. ISACA. https://www.isaca.org/credentialing/cism

ISC2. (2024). *Certified Information Systems Security Professional (CISSP)*. ISC2. https://www.isc2.org/Certifications/CISSP

ISO. (2013a). *ISO/IEC 27001 - Requirements for continually improving an information security management system*. https://www.iso.org/standard/54534.html

ISO. (2013b). *ISO/IEC 27002 - Selection, implementation and management of controls* https://www.iso.org/standard/54533.html

ISO. (2018). *ISO/IEC 27000 - Overview of information security management systems (ISMS)*. https://www.iso.org/standard/73906.html

ITU. (2008). Overview of Cybersecurity. *Rec. ITU-T X.1205 (04/2008)*

Iyengar, P. (2021). *Boards Are Driving Digital Deeper Into the Business*. Gartner.

Jensen, M. L., Durcikova, A., & Wright, R. T. (2021). Using susceptibility claims to motivate behaviour change in IT security. *European Journal of Information Systems, 30*(1), 27-45. 10.1080/0960085X.2020.1793696

Jensen, M. L., Wright, R. T., Durcikova, A., & Karumbaiah, S. (2022). Improving Phishing Reporting Using Security Gamification [Article]. *Journal of Management Information Systems, 39*(3), 793-823. 10.1080/07421222.2022.2096551

Jiawen, Z., Gengzhong, F., Huigang, L., & Kwok-Leung, T. (2023). How Do Paternalistic Leaders Motivate Employees' Information Security Compliance? Building a Climate and Applying Sanctions [Article]. *Journal of the Association for Information Systems, 24*(3), 782-817. 10.17705/1jais.00794

Kam, H. J., Ormond, D. K., Menard, P., & Crossler, R. E. (2022). That's interesting: An examination of interest theory and self-determination in organisational cybersecurity training [Article]. *Information Systems Journal, 32*(4), 888-926. 10.1111/isj.12374

Kappelman, L., Johnson, V. L., Maurer, C., Guerra, K., McLean, E., Torres, R., Snyder, M., & Kim, K. (2020). The 2019 SIM IT Issues and Trends Study [Article]. *MIS Quarterly Executive, 19*(1), 69-104. 10.17705/2msqe.00026

Kayworth, T., & Whitten, D. (2010). EFFECTIVE INFORMATION SECURITY REQUIRES A BALANCE OF SOCIAL AND TECHNOLOGY FACTORS [Article]. *MIS Quarterly Executive, 9*(3), 163-175.

Kemmerer, R. A. (2003, 3-10 May 2003). Cybersecurity. 25th International Conference on Software Engineering, 2003. Proceedings.

Kormos, C., POC, L. A. G., Givans, N., & Bartol, N. (1999). Using security metrics to assess risk management capabilities. National Information Systems Security Conference.

Kosutic, D., & Pigni, F. (2021). Cybersecurity: investing for competitive outcomes. *Journal of Business Strategy, 43*(1), 28-36. 10.1108/JBS-06-2020-0116

Kothari, C. R. (2004). *Research methodology methods & techniques* (2nd rev. ed.). New Age International P Ltd., Publishers.

Larsen, K. R., Lukyanenko, R., Mueller, R. M., Storey, V. C., VanderMeer, D., Parsons, J., & Hovorka, D. S. (2020, 2020//). Validity in Design Science Research. Designing for Digital Transformation. Co-Creating Services with Citizens and Industry, Cham.

Lee, C. H., Geng, X., & Raghunathan, S. (2016). Mandatory Standards and Organizational Information Security. *Information Systems Research, 27*(1), 70-86. 10.1287/isre.2015.0607

Leech, T. J., & Hanlon, L. C. (2017). *Board Cyber Risk Oversight*. John Wiley & Sons, Inc. 10.1002/9781119309741.ch2

Lennon, E. (2003). *IT Security Metrics*. (iTL Bulletin, Issue. NIST. NIST.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7*, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Liu, C.-W., Huang, P., & Lucas, H. C. (2020). Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. *Journal of Management Information Systems, 37*(3), 758-787. 10.1080/07421222.2020.1790190

Longo, J. (2023). *ESG: Major change is underway, and we need to be ready*. ASIC. https://asic.gov.au/about-asic/news-centre/speeches/esg-major-change-is-underway-and-we-need-to-be-ready/

Lund, F., & Richter, W. (2021). *Boards and Cybersecurity - How boards should prepare for the rising cybersecurity threat*. McKinsey. McKinsey.

Mandy, C., Olyaei, S., & Proctor, P. (2021). *Metrics to Prove You CARE About Cybersecurity*. Gartner.

Manson, N. J. (2006). Is operations research really research? *ORiON, 22*(2), 155-180.

McLaughlin, M.-D., & Gogan, J. (2018). Challenges and Best Practices in Information Security Management [Article]. *MIS Quarterly Executive, 17*(3), 237-262.

McNulty, E., Lee, J. E., Boni, B., Coghlan, J. P., & Foley, J. (2007). Boss, I Think Someone Stole Our Customer Data [Case Study]. *85*, 37-50.

Mehrizi, M. H. R., Nicolini, D., & Mòdol, J. R. (2022). HOW DO ORGANIZATIONS LEARN FROM INFORMATION SYSTEM INCIDENTS? A SYNTHESIS OF THE PAST, PRESENT, AND FUTURE [Article]. *MIS Quarterly, 46*(1), 531-590. 10.25300/MISQ/2022/14305

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *Journal of Management Information Systems, 34*(4), 1203-1230. 10.1080/07421222.2017.1394083

Merriam, W. (2013). *Webster's American English Dictionary*. Federal Street Press.

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security, 120*, 102820. https://doi.org/10.1016/j.cose.2022.102820

Möller, F., Schoormann, T., Strobel, G., & Hansen, M. R. P. (2022). Unveiling the Cloak: Kernel Theory Use in Design Science Research. ICIS.

NACD. (2020). *Cyber-Risk Oversight 2020*.

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices to situated practices. *European Journal of Information Systems, 26*(1), 1-20. 10.1057/s41303-016-0025-y

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST. (2019). *Computer Security Resource Center (CSRC)*. NIST. https://csrc.nist.gov/glossary/term/Cyber_Security

Nolan, R., & McFarlan, F. W. (2005). Information technology and the board of directors. *Harvard business review, 83*(10), 96-157.

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research.

Olyaei, S., & Mandy, C. (2022). *Predicts 2022: Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem*. Gartner.

Olyaei, S., Thielemann, K., Addiscott, R., & Pratap, K. (2021). *Predicts 2021: Cybersecurity Program Management and IT Risk Management*. Gartner. Gartner.

Olyaei, S., & Wheatman, J. (2020). *Craft Effective Responses to the Board's 5 Cybersecurity and Technology Risk Management Questions*. Gartner.

Olyaei, S., & Wheatman, J. (2022). *Five Board Questions That Security and Risk Leaders Must Be Prepared to Answer*. Gartner.

OpenGroup. (2017). *Open Information Security Management Maturity Model (O-ISM3), Version 2.0*. https://publications.opengroup.org/standards/security/c17b
OPTUS. (2023). *Optus notifies customers of cyberattack compromising customer information*. Optus. https://www.optus.com.au/about/media-centre/media-releases/2022/09/optus-notifies-customers-of-cyberattack
Orlikowski, W. J., & Baroudi, J. J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research, 2*(1), 1-28. 10.1287/isre.2.1.1
Parenty, T. J., & Domet, J. J. (2019). Sizing Up Your Cyberrisks [Article]. *Harvard Business Review - HBR, 97*(6), 102-109.
Parsons, J., Tuunanen, T., Venable, J., Donnellan, B., Helfert, M., & Kenneally, J. (2016). PADRE: A Method for Participatory Action Design Research. In (Vol. 9661, pp. 19-36). Springer International Publishing AG. 10.1007/978-3-319-39294-3_2
Payne, S. (2006). *A Guide to Security Metrics*. S. Institute. SANS Institute.
PCI. (2018a). *Data Security Council - Requirements and Security Assessment Procedures*. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1620271800501
PCI. (2018b). *Data Security Standard*. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1620271800501
Pearlson, K., & Novaes Neto, N. (2022, 4 March 2022). 7 Pressing Cybersecurity Questions Boards Need to Ask. *Harvard business review*.
Pearlson, K., Schwartz, J., Sposito, S., & Arbisman, M. (2022). How Verizon Media Built a Cybersecurity Culture [Article]. *MIS Quarterly Executive, 21*(2), 165-183. 10.17705/2msqe.00064
Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2008). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems, 24*(3), 45.
Peppard, J., Reich, B., & Mocker, M. (2023). Special Issue Editorial: Boards of Directors and the Governance of Technology [Article]. *MIS Quarterly Executive, 22*(4), xvii-xxviii.
Pienta, D., Thatcher, J. B., & Johnston, A. (2020). Protecting a whale in a sea of phish. *Journal of Information Technology, 35*(3), 214-231. 10.1177/0268396220918594
Press, C. (2011). *Cambridge English Dictionary*. Cambridge University Press.
Proctor, P. (2020). Outcome-Driven Metrics for Cybersecurity in the Digital Era. https://www.gartner.com/document/3980892?ref=solrAll&refval=287508943
Proctor, P. (2021a). *Cybersecurity Must Be Treated as a Business Decision*. Gartner.
Proctor, P. (2021b). *An Outcome-Driven Approach to Cybersecurity Improves Executive Decision Making*. Gartner.
Proctor, P. (2021c). *Outcome-Driven Metrics for Cybersecurity in the Digital Era*. Gartner.
Proctor, P., & Shankel, S. (2023). *Four Steps to Develop Outcome-Driven Metrics for Cybersecurity*. Gartner.
Proudfoot, J. G., Madnick, S., Cram, W. A., & Coden, M. (2023). The Importance of Board Member Actions for Cybersecurity Governance and Risk Management [Article]. *MIS Quarterly Executive, 22*(4), 235-250. 10.17705/2msqe.00084
Rantos, K., Fysarakis, K., & Manifavas, C. (2012). How Effective Is Your Security Awareness Program? An Evaluation Methodology. *Information security journal., 21*(6), 328-345. 10.1080/19393555.2012.747234
Rout, D. (2015). Developing a Common Understanding of Cybersecurity. *ISACA JOURNAL Volume 6*.
Safi, R., Browne, G. J., & Jalali Naini, A. (2021). Mis-spending on information security measures: Theory and experimental evidence. *International Journal of Information Management, 57*, 102291. https://doi.org/10.1016/j.ijinfomgt.2020.102291
Savola, R. (2007). *Towards a taxonomy for information security metrics* Proceedings of the 2007 ACM workshop on Quality of protection, Alexandria, Virginia, USA. https://doi-org.ezproxy.lib.uts.edu.au/10.1145/1314257.1314266
Savola, R. (2008). A Novel Security Metrics Taxonomy for R&D Organisations. ISSA.

SCC/SEC. (2023, 15 March 2023). *SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*. https://www.sec.gov/news/press-release/2023-139
Scholtz, T. (2021). *How to Communicate the Value of Information Security in Business Terms*. Gartner.
Schuetz, S. W., Benjamin Lowry, P., Pienta, D. A., & Bennett Thatcher, J. (2020). The Effectiveness of Abstract Versus Concrete Fear Appeals in Information Security. *Journal of Management Information Systems, 37*(3), 723-757. 10.1080/07421222.2020.1790187
ScienceDirect. (2021). *Science Direct.* Reed Elsevier Inc.].
Scopus. (2008). *Scopus Database*. Elsevier Scientific Publishing Company.
Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). ACTION DESIGN RESEARCH [Essay]. *MIS Quarterly, 35*, 37-56. 10.2307/23043488
Shackelford, S. J., Russell, S., & Haut, J. (2015). Bottoms up: A comparison of voluntary cybersecurity frameworks. *UC Davis Bus. LJ, 16*, 217.
Shariffuddin, N., & Mohamed, A. (2020). *IT Security and IT Governance Alignment: A Review* Proceedings of the 3rd International Conference on Networking, Information Systems & Security, Marrakech, Morocco. https://doi-org.ezproxy.lib.uts.edu.au/10.1145/3386723.3387843
Silic, M., & Lowry, P. B. (2020). Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance. *Journal of Management Information Systems, 37*(1), 129-161. 10.1080/07421222.2019.1705512
Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2023). A pathway model to five lines of accountability in cybersecurity governance. *International Journal of Accounting Information Systems, 51*, 100642. https://doi.org/10.1016/j.accinf.2023.100642
Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems, 44*, 100548. https://doi.org/10.1016/j.accinf.2021.100548
Smith, T. J., Higgs, J. L., & Pinsker, R. E. (2019). Do Auditors Price Breach Risk in Their Audit Fees? [Article]. *Journal of Information Systems, 33*(2), 177-204. 10.2308/isys-52241
Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009
Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2016). SECURQUAL: An Instrument for Evaluating the Effectiveness of Enterprise Information Security Programs [Article]. *Journal of Information Systems, 30*(1), 71-92. 10.2308/isys-51257
Stevenson, A. (2010). *Oxford dictionary of English* (3rd ed. / edited by Angus Stevenson. ed.). Oxford University Press.
SWIFT. (2020). *SWIFT Customer Security Controls Framework (CSCF)* https://www.swift.com/myswift/customer-security-programme-csp/security-controls#:~:text=The%20SWIFT%20Customer%20Security%20Controls%20Framework%20(CSCF)%20is%20composed%20of,baseline%20for%20the%20entire%20community.&text=The%20advisory%20controls%20are%20based,recommends%20all%20users%20to%20implement.
Taherdoost, H. (2022). Cybersecurity vs. Information Security. *Procedia Computer Science, 215*, 483-487. https://doi.org/10.1016/j.procs.2022.12.050
Torabi, S. A., Rezaei Soufi, H., & Sahebjamnia, N. (2014). A new framework for business impact analysis in business continuity management (with a case study). *Safety Science, 68*, 309-323. https://doi.org/10.1016/j.ssci.2014.04.017
Urquhart, C., Lehmann, H., & Myers, M. D. (2010). Putting the 'theory' back into grounded theory: guidelines for grounded theory studies in information systems. *Information systems journal (Oxford, England), 20*(4), 357-381. 10.1111/j.1365-2575.2009.00328.x
Vaishnavi, V., & Kuechler, B. (2008). On theory development in design science research: anatomy of a research project. *European Journal of Information Systems, 17*(5), 489-504. http://dx.doi.org/10.1057/ejis.2008.40
Vaishnavi, V., & Kuechler, W. (2015). *Design science research methods and patterns : innovating information and communication technology* (Second edition. ed.). CRC Press.

Vedadi, A., & Warkentin, M. (2020). Can Secure Behaviors Be Contagious? A Two-Stage Investigation of the Influence of Herd Behavior on Security Decisions. *Journal of the Association for Information Systems, 21*(2), 428-459. http://dx.doi.org/10.17705/1jais.00607

Vijay, V., & Kuechler, B. (2021). *Design Science Research in Information Systems*.

Vom Brocke, J., Hevner, A., & Maedche, A. (2020). Introduction to design science research. *Design science research. Cases*, 1-13.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Walls, A., Perkins, E., & Weiss, J. (2014). *Definition: cybersecurity*. Gartner. https://www.gartner.com/document/2510116?ref=solrAll&refval=285974841

Walls, J. G., Widmeyer, G. R., & El Sawy, O. A. (1992). Building an Information System Design Theory for Vigilant EIS [Article]. *Information Systems Research, 3*(1), 36-59. 10.1287/isre.3.1.36

Walton, S., Wheeler, P. R., Zhang, Y., & Zhao, X. (2021). An Integrative Review and Analysis of Cybersecurity Research: Current State and Future Directions [Article]. *Journal of Information Systems, 35*(1), 155-186. 10.2308/ISYS-19-033

Wang, Q., Ngai, E. W. T., Pienta, D., & Thatcher, J. B. (2023). Information Technology Innovativeness and Data-Breach Risk: A Longitudinal Study [Article]. *Journal of Management Information Systems, 40*(4), 1139-1170. 10.1080/07421222.2023.2267319

Warner, M. (2012). Cybersecurity: A Pre-history. *Intelligence and National Security, 27*(5), 781-799. 10.1080/02684527.2012.708530

WEF. (2021). *Principles for Board Governance of Cyber Risk*. (INSIGHT REPORT, Issue. World Economic Forum. https://www.weforum.org/reports/136f100d-381a-4b09-a891-de2299144992

Wilkes, G. A., & Krebs, W. A. (1995). *Collins concise dictionary* (3rd ed. / special Australian consultants G.A. Wilkes, W.A. Krebs. ed.). HarperCollins.

Winnefeld Jr, J. A. S., Kirchhoff, C., & Upton, D. M. (2015). Cybersecurity's human factor: Lessons from the Pentagon [Article]. *Harvard Business Review HBR, 93*(9), 86-17.

Witty, R., & Hoeck, M. (2022). *How to Prepare for and Respond to Business Disruptions After Aggressive Cyberattacks*. Gartner.

Wolff, J. (2016). Perverse Effects in Defense of Computer Systems: When More Is Less. *Journal of Management Information Systems, 33*(2), 597-620. 10.1080/07421222.2016.1205934

Yang, S. O., Hsu, C., Sarker, S., & Lee, A. S. (2017). Enabling Effective Operational Risk Management in a Financial Institution: An Action Research Study. *Journal of Management Information Systems, 34*(3), 727-753. 10.1080/07421222.2017.1373006

Yeoh, W., Wang, S., Popovič, A., & Chowdhury, N. H. (2022). A systematic synthesis of critical success factors for cybersecurity. *Computers & Security, 118*, 102724. https://doi.org/10.1016/j.cose.2022.102724

Zhao, X., Zhao, J., Jiang, X., Zhang, X., & Zhang, W. (2019). Construction and Security Measurement of Cybersecurity Metrics Framework Based on Network Behavior. *Journal of Physics: Conference Series, 1302*, 022069. 10.1088/1742-6596/1302/2/022069

Zhuang, Y., Choi, Y., He, S., Leung, A. C. M., Lee, G. M., & Whinston, A. (2020). Understanding Security Vulnerability Awareness, Firm Incentives, and ICT Development in Pan-Asia. *Journal of Management Information Systems, 37*(3), 668-693. 10.1080/07421222.2020.1790185