7-4-2022

A Data Driven Approach to Board Cybersecurity Governance

Sarv Girn
University of Technology Sydney, sarv.girn@uts.edu.au

A Data Driven Approach to Board Cybersecurity Governance

Completed Research Paper

Sarv Girn
University of Technology Sydney (UTS)
Faculty of Engineering and IT, Ultimo, NSW, Australia 2007
sarv.girn@uts.edu.au

Abstract

The importance of managing cybersecurity has increased as the dependency upon online digital services has grown, and as threats to the digital economy have increased in sophistication and volume. Senior executives and board directors remain apprehensive when it comes to governing the quality of their organization's cybersecurity. Whilst there has been a growth in awareness in recent years, this has not provided terminology or metrics that allow them to confidently govern cybersecurity.

A systematic literature review demonstrates there is limited research targeted at this audience. The more technical cybersecurity and risk professionals are better served.

Further research is warranted so that a practical cybersecurity model aimed at senior executives and board directors is defined. This would be akin to financial reporting that frames the financial posture in terms of cash flow, assets, and liabilities. The model would be extensible and enable improvements through further research as cybersecurity evolves.

Keywords: executive, board director, cybersecurity metrics, lexicon, governance, assurance

Introduction

Cybersecurity refers to the organizational capability that deals with the protection of digital systems or related assets from external and internal threats. It is defined as 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" (Craigen et al. 2014). Cybersecurity is often linked to the management of confidentiality, integrity, and availability risks of digital systems or services (Cains et al. 2021). The importance of managing cybersecurity risk has become increasingly more relevant as the dependency upon online digital services has grown for many organizations (Guthrie et al. 2021). This has been compounded with increased sophistication of threats that impact the confidentiality, integrity and availability of systems (Pienta et al. 2020), with the corresponding impact to clients, shareholders and other stakeholders (Li et al. 2019). For instance, recent examples of impact include (Smith 2020) and (Ward 2021) where consumers were impacted by cyberattacks with the inevitable cost to the relevant company to remediate and manage brand damage and reputation. In addition, regulators are initiating criminal charges upon organizations and individuals where cybersecurity has not been managed in line with expectations, (ASIC 2020). Whilst there is an abundance of focus from government and industry bodies on cybersecurity strategies, standards and guidelines; senior executives and board directors remain apprehensive when it comes to governing the posture of their organization's security. An example of this is a survey of financial institutions (ASIC 2019) which found that only 50% of boards are somewhat confident of their company

being properly secured against cyber-attacks. There are a large number of articles to increase awareness amongst senior executives and boards through the efforts of organizations such as the Australian Institute of Company Directors (AICD 2022) . However, this has not provided a business lexicon and supporting metrics to allow them to govern cybersecurity in a data driven manner. The guidance for boards remains purely at a conceptual level covering the principles directors should follow in governing cybersecurity. An example of this is (WEF 2021) where the report frames principles to adopt; however it falls short of providing guidance on how they do this and what metrics they can use to track progress of this important imperative.

Research and guidance are required so that akin to financial frameworks (such as cash flow, balance sheet, and profit/loss statements) the cybersecurity posture can be clearly understood through a framework of data driven metrics. The interplay across the cybersecurity ecosystem is depicted in Figure 1, where the heart of the challenge is the Direction and Assurance interchange between cybersecurity governance and cybersecurity implementation, in a lexicon that can be understood by upstream and downstream participants. This is in effect a translation layer of terminology between these stakeholders.

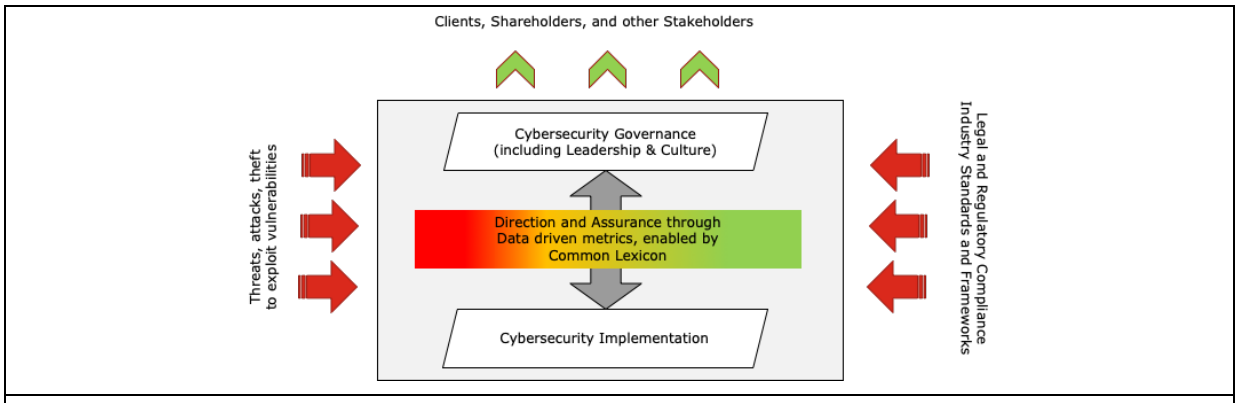

Figure 1: The gap between cybersecurity governance and implementation

Research Question (RQ):

This research is a first step to understanding the frameworks in place that cover metrics and lexicon for the senior executive and board director audience when governing cybersecurity. This paper focusses on the following main research question:

RQ. What cybersecurity artefacts are available for the senior executive and board director audience to help in the governance of cybersecurity risk?

This is further broken down into two sub-questions.

RQ1. What data driven metrics have been identified for senior executives and board directors for determining the health of cybersecurity in an organization?

RQ2. What business lexicon models are available for senior executives and board directors to better understand the technical terminology used in the implementation of cybersecurity?

This research has conducted a detailed systematic literature review (SLR) (Okoli and Schabram 2010) to identify existing literature targeted at helping senior executives and board directors in cybersecurity governance. This work represents a foundation for further research into this topic. Furthermore, theories such as the common ground theory, kernel theory, and rational choice theory have been identified as relevant for future research in this field of work. These should be applied to the research questions to assist in identification and abstraction (Fischer et al. 2010) of classes of the right data metrics and lexicon that bridges business and technical stakeholders. Specifically, the Kernel theory would guide this research to ensure the appropriate design of relevant artefacts in the executive information system, whilst Common ground theory will play a vital role in framing the appropriate bridging lexicon. Independence from the underlying state of cybersecurity (to avoid coverage bias in metric design that may be not reflect the end to end environment) will be informed by the Rational choice theory. Feedback on the use of these theories to

such research problems is expected and the research itself would contribute to the gap seen in industry and literature. The use and expected outcomes are further covered in the Contribution section.

This paper is organized as follows. Firstly, it provides the conceptual foundation and research background including the research problem. Secondly it discusses the research method and results. Finally, it outlines the key insights and contributions before concluding.

Conceptual Foundation and Research Background

Conceptual Foundation

The term "Cybersecurity" is used in many contexts and often has different meaning to authors and those that need to then interpret such writings in their work. If we examine dictionary sources, academic literature, and then industry practices, we can identify a range of common elements in the definitions.

When looking at English dictionary sources for the definition of cybersecurity, a common theme is to state cybersecurity as being the act of protecting data belonging to individuals and organizations from criminal or unauthorized systems access, (Merriam 2013; Stevenson 2010; Wilkes and Krebs 1995). Definitions do not limit protection to specific control areas across people, processes, or technology. They are inclusive of all dimensions, and could include things like 'culture' and 'awareness'. This makes the cyber security field very broad.

Academic literature has taken a more precise view of the definition, however there still remains some level of variability. In many cases authors have stated their assumed definition upfront to avoid ambiguity, (Azmi et al. 2018). Definitions are highly variable and that the multidimensions of cybersecurity are not captured in any existing description (Craigen et al. 2014). The authors here 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 Software Engineering Institute (Cebula et al. 2014) breaks down cybersecurity into a taxonomy consisting of four dimensions; actions of people, systems failures, process failures and external events. This brings a more defined scope, though softer aspects related to people and their behavior seem to be less prominent and are only be covered lightly under failed internal processes. Another aspect of the definition of cybersecurity is the concept 'information security'. This relationship is framed by (von Solms and van Niekerk 2013) where the authors argue that whilst there is 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.

Industry definitions in recent years have encompassed the people aspects and framed the confidentiality, integrity and availability of the data. This includes, (CISA 2019) and (CISCO 2021) where cybersecurity is defined as the 'practice of protecting systems, networks, and programs from digital attacks'. Further, (Rout 2015) frames 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. Also, (NIST 2019) 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. Technology research company Gartner (Walls et al. 2014) also confirms this confusion, and has offered a definition that is grounded in military terminology as, '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'.

Examination of the definitions of cybersecurity across dictionary, academic and industry sources has revealed there is no one agreed definition. However, there is a convergence in views, whereby cybersecurity is seen not just limited to the domain of the technology or the processes required to maintain it. It also encompasses other aspects, such as human behavior and culture. The breadth of concepts found in dictionary, academic and industry cybersecurity definitions examined have been synthesized and are depicted in Figure 2.

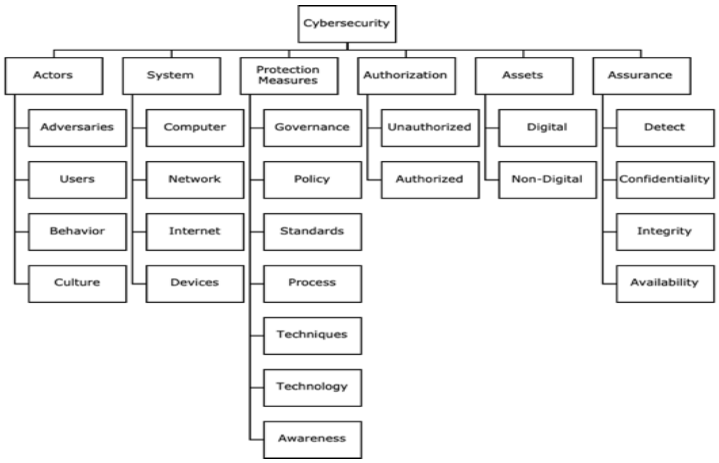

Figure 2: Concepts in Cybersecurity Definitions

The fact that industry and academic sources cannot agree on a single definition, and that the various definitions identified offer different (yet relevant) concepts, are both very pertinent to cybersecurity governance. It is this variability, and the lack of an agreed single universal definition that makes governance of cybersecurity for senior executives and board directors harder in what is already a complex and evolving field for them.

Given this inherent challenge and to avoid ambiguity, this paper defines cybersecurity to be "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'. Furthermore, the importance of taking a data driven approach to measuring cybersecurity effectiveness becomes critical in order to overcome the challenges outlined in the varying definitions. A data-driven approach would clearly spell out the metrics that relate to the definition, and also would have associated lexicon to explain the meaning of each data element. This would minimize the ambiguity in breadth and depth of the definition, and also offer a basis for extension as the cybersecurity field evolves further to include other concepts.

Research Background

Following on from the conceptual foundation of cybersecurity, it becomes important to understand how cybersecurity is governed in terms of overseeing and directing investments and resources towards the desired state. This oversight, or 'governance' has been explained by (Allen 2005) as 'setting clear expectations for the conduct (behaviors and actions) of the entity being governed, and directing, controlling and strongly influencing the entity to achieve these expectations'. In context of 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).

Oversight of cybersecurity starts at the board level, with setting of business strategy and goals, along with defining and embedding a risk framework. Whilst a two-way discussion occurs with management, the final approval and setting the tone of the strategy sits with the board. For government entities, this follows a similar approach, with relevant local, state and federal ministerial teams. The cybersecurity agenda is an inherent part of this process in mature organizations so that it is embedded in strategic and risk roadmaps, and 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, literature falls short of identifying metrics and mechanisms to access the alignment from an executive or board standpoint. Whilst (AlGhamdi et al. 2020) and also (Bruin and Solms 2016) cite the necessity for top-level management and board level focus to drive maturity, they fall short of providing specific dimensions to track and report upon. Regulators also have in recent years included specific requirements for boards. An example of this is the Australian Prudential Regulation Authority (APRA), which is an independent statutory authority that supervises and

regulates banking, insurance and superannuation organizations in Australia. APRA has mandated a prudential standard on Information Security, CPS234 (APRA 2019), stating 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 a data driven approach of metrics that can be used to fulfil this accountability with ease. Regulated entities are having to infer their own specific frameworks to provide this assurance. This issue is compounded as focus has increased to regulated-organizations being asked to provide downstream assurances on their suppliers, each of which have a different way of measuring the cybersecurity posture.

As the importance of cybersecurity governance has become more critical for organizations (Haislip et al. 2021) and (Walton et al. 2021), a range of frameworks and standards have evolved to guide the implementation of governance processes and controls. These stem from literature related to Information Technology (IT) governance, with appropriate extensions added for cybersecurity risk. The Information Security Governance and Management (ISGM) framework (Carcary et al. 2016) has its basis from COBIT (Harmer 2013) and the Open Group (OpenGroup 2017). Similarly, various security standards from ISO, such as (ISO 2018), (ISO 2013a) and (ISO 2013b) have framed key processes and controls expected in best practice organizations. A number of industry specific frameworks have also been released that apply to regulated organizations. This is not limited to financial services, which has historically been regulated on operational risk matters for many years. Regulated entities, have faced increasing scrutiny on the posture of their cybersecurity given the impact that can occur to the broader economy from a breach of security. The energy sector is one case in point (AEMO 2019). This has its basis on a range of ISO/IEC and NIST standards (NIST 2018), and focus on maturity of key processes that must be in place for sound cybersecurity management. These include aspects such as asset, change and configuration management, identity and access management, and event and incident response, including continuity of operations. The target audience for this framework are risk and security practitioners. More broadly, the Australian Securities and Investment Commission (ASIC), which regulates all companies across Australia, has published a range of standards for companies on good cyber resilience, including (ASIC 2015) which covers broad areas to look into in the form of a health check. It has over time increased its focus on this through additional reviews of the corporate sector to highlight good practices and areas to improve in (ASIC 2019). Furthermore, the Australian Stock Exchange (ASX) and ASIC also conducted a health check of the top ASX 100 companies and published its findings (ASX/ASIC 2017). This report concluded a range of findings, including:

- Only 34% of boards have a clearly defined risk appetite statement for cybersecurity;
- Only 50% of boards are somewhat confident that their company is properly secured against cyber-attacks (43% appear confident); and
- Only 11% of boards have a clear understanding of where the company's key information and data assets are shared with third parties.

These insights clearly show there more to be done to increase the knowledge and awareness amongst senior leadership that govern enterprises. Further, it should be noted regulators are now initiating criminal charges against organizations that demonstrate poor practices in cybersecurity such as (ASIC 2020). Such developments and directions clearly raise the importance of good cybersecurity governance in the industry.

Related Work and Problem Statement

There are many artefacts to assist in governing the cybersecurity posture of organizations in terms of strategies, policies, guidelines, processes and standards. These begin with general government guidance such as that from (ACSC 2021), and industry bodies such as (AustCyber 2021). More detail is then present in ISM/ISO/NIST standards from international bodies. Some regulated industries have extended these to their own specific standards in order to stress key elements of these; and often compliance is required for the generic and industry specific set. This brings about several themes that create challenges:

- Cybersecurity standards pose a need for intricate understanding when making the choice of which standard(s) to use as a baseline target – practitioners often have differing views on this; and

- The language of these standards is aimed at a target audience of the risk and security practitioner, not a business executive who may be governing the organization.

By way of example, Table 1 outlines material standards in financial services in Australia. Whilst the mandated ones are not an issue, it is the selection of others that becomes difficult. The subsequent assurance that follows becomes harder, when the baseline can vary across organizations.

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 card payment data	Y (if processing card data)	(PCI 2018)
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 1: Cybersecurity Standards for Financial Services (Australia)

The issue becomes even more visible when one examines the target audience of these frameworks and standards. Table 2 below has been produced through examination of the detail in each artefact, the skills and experience required to comprehend this, and the stated intent of the artefact. From this it is clear that the very user group (Board and CxO) that is being held accountable for setting the direction and governing the cybersecurity risk profile is the one that is served least in these artefacts.

Artefact[1]	**Primary Target Audience**						
	Board of Directors	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 2: Primary Target Audience for Cybersecurity Artefacts

When examining literature on cybersecurity governance there is limited knowledge to provide guidance for the senior executive and board director audience, in a language, granularity, and style they can understand

[1] Artefact in this instance is assumed to be a standard, framework or accreditation related to Cybersecurity

and apply. Whilst frameworks such as COBIT (Harmer 2013) provide a broad outline of key processes for managing technology risk, they fall short of specifying measures, indicators and red-flags for this audience. The terminology in many of the ISO/IEC, NIST and CISM frameworks is technical in nature, and there is a lack of lexicon that maps this to the language of the senior executive and board director audience. This translation is often left to various risk and audit SMEs who are reliant on bespoke interpretation in each firm, without any consistency across the industry. Surveys of this audience (ASX/ASIC 2017) demonstrate the lack of understanding when only 34% of the companies in the ASX 100 have cybersecurity risk appetite clearly defined and understood, and 'most respondents have either not defined or only partially defined their cyber risk appetite.' A model that maps downstream technical lexicon to business language used by senior stakeholders upstream is lacking in literature. Whilst (Cebula et al. 2014) frames taxonomy that could be applied to some areas of cybersecurity, it stops short of including people, culture and behavioral aspects of cybersecurity. An integrated model for senior business leaders consisting of taxonomy and metrics is absent in literature. If this was present, it would encourage a data driven approach to cybersecurity governance. The lack of an integrated model is also seen from an industry perspective, whereby Gartner Research (Proctor 2021a) 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 research background and problem statement has provided early indication for the need to seek out existing literature on the research question. Namely, *what cybersecurity artefacts are available for the senior executive and board director audience to help in the governance of cybersecurity risk?*

This primary question then directs two sub-questions. First to seek insights on, *what data driven metrics have been identified for senior executives and board directors for determining the health of cybersecurity in an organization?* Second to seek insights on, *what business lexicon models are available for senior executives and board directors to better understand the technical terminology used in the implementation of cybersecurity?*

The range of challenges faced by senior executives and board directors are visually depicted in Figure 3.

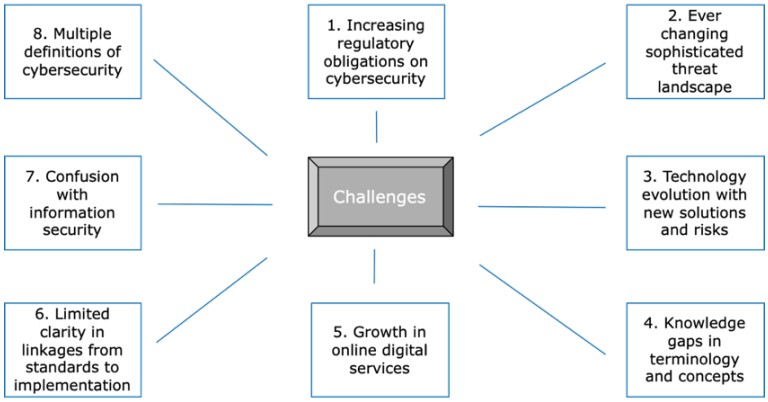

Figure 3: Challenges faced by Executives and Board Directors

A sample of the key reference points for these challenges are represented in Table 3.

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

Challenge #	Literature references
8 – Multiple definitions of cybersecurity	(Cains et al. 2021); (Craigen et al. 2014)

Table 3: Key References for challenges faced by Executives and Board Directors

Research Method

The research followed the systematic literature review (SLR) method (Okoli and Schabram 2010). At the heart of answering the research question and the sub-questions, was to understand and frame the extent to which senior executives and board directors were targeted in the form of a framework of metrics and lexicon, that assisted them in the governance of cybersecurity.

The research method focused on searching a specified set of journals, some reputable industry sources that could compliment these papers, and then analysis and synthesis of the material into key concepts covered for the target audience.

Sources of literature

The scope of this research is limited to the AIS Basket of Eight Information Systems (IS) Journals (1-8), along with a select number of additional relevant journals (9-11) as noted below:

1. European Journal of Information Systems (EJIS)
2. Information Systems Journal (ISJ)
3. Information Systems Research (ISR)
4. Journal of Association for Information Systems (JAIS)
5. Journal of Information Technology (JIT)
6. Journal of Management Information Systems (JMIS)
7. Journal of Strategic Information Systems (JSIS)
8. MIS Quarterly (MISQ)
9. International Journal of Information and Management (IJIM)
10. Journal of Information Systems (JIS)
11. MIS Quarterly Executive (MISQE)

In addition, the following key mainstream business/industry sources have also been examined (by searching their relevant websites and portals) to compliment the academic research articles:

1. Gartner
2. Harvard Business Review
3. McKinsey

Search terms

The review included identifying relevant papers since 1 January 2016 (last 5 years) to 1 November 2021 that bridge business and technical lexicon in cybersecurity, and offer a series of metrics to track cybersecurity risk. Table 4 outlines the search terms used to identify and examine candidate papers and then filter down to frame key literature and insights. The cybersecurity dimensions originate from various security frameworks (ISO 2018; NIST 2018) as terminology typically referred to in governance.

Cybersecurity Dimension	Primary search domain	Secondary search domains / synonyms	Search Reference (SR) #
Leadership	"cybersecurity" or "information security"	"governance" or "reporting" or "assurance" or "leadership"	SR#1
Assurance	"cybersecurity" or "information security"	"health" or "maturity" or "index"	SR#2
Benchmarking	"cybersecurity" or "information security"	"metrics" or "ratios" or "indicators"	SR#3

Cybersecurity Dimension	Primary search domain	Secondary search domains / synonyms	Search Reference (SR) #
Terminology	"cybersecurity" or "information security"	"lexicon" or "ontology" or "concepts"	SR#4
Stakeholders	"cybersecurity" or "information security"	"directors" or "boards" or "executives"	SR#5
Regulation	"cybersecurity" or "information security"	"standards" or "regulation" or "regulator"	SR#6

Table 4: Search terms applied to identify Candidate Papers

The rational for the primary search domain stems from a gradual shift (Warner 2012) of the terminology from "information security" towards "cybersecurity", along with a lack of consistency seen in the use of these terms in literature and industry, (Craigen et al. 2014). The secondary search domains represent synonyms to the cybersecurity dimension being sought in literature. These synonyms are based on common lexicon often used with the cybersecurity dimension by business stakeholders in documents such as board papers, audit reports and compliance statements. The use of several synonyms provides a fuller coverage of the cybersecurity dimension and reduces risk from differing terms being used in literature.

Given the research question is targeted at a senior executive and board director audience, only literature for this stakeholder group was screened for inclusion. In addition, literature that focused on bridging the language divide between this audience and cybersecurity technical community was included. Literature that is targeted at the technical audience alone and would not provide a translation layer or framework for consumption by business executives or board directors was excluded. The same screening approach was applied to journal and industry sources.

Filtering stages

The identification and filtering of papers followed a series of stages as follows:

1. Stage 1 – identified papers matching the stated search terms in each journal and industry source, without any form of filtering. The output is termed 'Stage 1' papers
2. Stage 2 – involved a review of Stage 1 papers by examining the title, abstract and skimming the papers for screening purposes. The skimming of the papers was necessary to identify even small but relevant insights. This stage filtered down the papers to 'Stage 2' papers.
3. Stage 3 – takes Stage 2 papers to more comprehensive analysis to identify those that provide useful knowledge in context to the problem statement. This includes removal of duplicate papers that appear in multiple search criteria. These are termed 'Stage 3' papers.
4. Stage 4 – examined Stage 3 papers and looked at References through examining the title, abstract, and skimming. The intention of this was to examine upstream references that may prove to be useful for the problem statement, which were not picked up in Stage 1.

Stage 3 & 4 papers have then been analyzed in order to synthesize key concepts, focus areas, gaps and insights for building future research and knowledge. The overall approach is depicted in Figure 5.

Results

The initial search results from Stage 1 revealed 2,628 papers from academic literature sources along with 549 papers from industry sources (websites/portals for the three organizations listed previously). However, upon filtering these through review of titles, abstract, and skim reading (with the same approach for academic and industry papers), this number reduced to 204 and 15 respectively in Stage 2. Stage 3, which involved a deeper review and also removal of duplicate papers led to 30 papers from academic literature (with no reduction in industry papers from the 15).

Following this, the upstream references in the papers from Stage 3 were examined through skimming of title, abstract and a high-level review. This led to an additional 9 papers being added which were not in the original set. The increase in papers is attributed to an identification of upstream papers that were outside

of the 5-year date horizon for the original search terms. Whilst not directly relevant for the research question, these papers did offer useful background reading to the topic; and as such were included in the counts and not discarded. The 39 papers from academic sources, and 15 from industry sources represented the total set of papers (54) relevant for the scope of research. Figure 5 depicts the approach and papers from each stage.

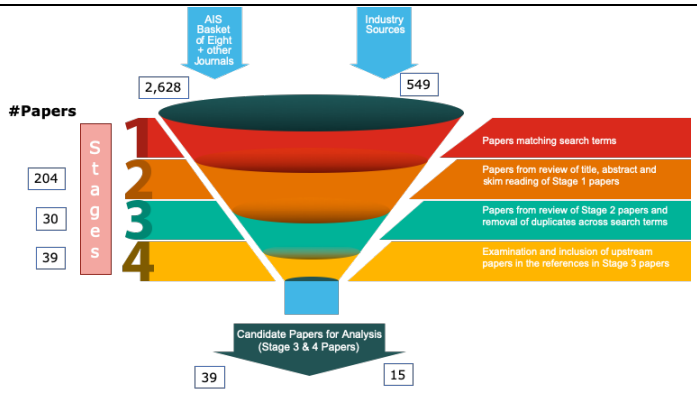

Figure 4: Approach and Results from each stage of Systematic Literature Review

The literature references from stage 4 are show in Figure 6, where the distinct lack of papers covering health, maturity, index, metrics, ratios or indicators (SR#2 and SR#3) is seen. There is also limited coverage of lexicon, ontology, or concepts (SR#4) to explain the terminology. However, there is good coverage of governance, reporting, assurance and leadership (SR#1) when it comes to the need and importance for oversight of cybersecurity. The coverage for executives and directors (SR#5) relates to principle level guidance and confirming the importance of their accountability.

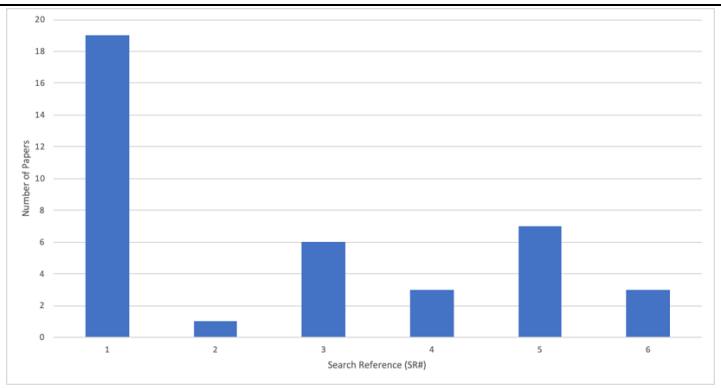

Figure 5: Summary of Literature References

Discussion

Given the relatively few papers found in the systematic literature review (54) it is evident the senior executive and board director audience is not well served in literature or industry sources. A detailed analysis and synthesis of these papers has revealed six conceptual themes that are evident with varying levels of coverage as outlined in Table 5. These conceptual terms are at a higher level than the secondary search domains/synonyms in Table 4 for the purposes of a general discussion. These originate from principle levels literature targeted at senior executives and board directors (CAQ 2018; CII 2016; WEF 2021).Given overlaps in papers, and unstructured nature of the descriptions in these, this analysis should be seen as directionally correct and not a precise form. The gaps are more pronounced in Reporting (limited coverage

of specific reporting frameworks), Assets (not specifically identified for targeted protection), and Lexicon (narrow coverage of terminology between business and technical audiences). Each of these conceptual themes are now discussed.

	Conceptual themes	Extent of coverage[2] (H, M, L)	Insights synthesised	# of Papers	References
1	Principles	H	Good coverage on foundational principles in setting the tone and approach for cybersecurity governance for executives and board directors. This includes the types of questions that should be asked to ascertain maturity.	11	(AICPA 2018) (Baxter et al. 2016) (CAQ 2018) (Clinton et al. 2020) (Cram et al. 2021) (Leech and Hanlon 2017) (Lee et al. 2016) (McLaughlin and Gogan 2018) (CII 2016) (WEF 2021) (Winnefeld Jr et al. 2015)
2	Accountability	M	The importance of the Board being cybersecurity accountable is a consistent theme, along with the CEO and executives collectively owning cybersecurity, not just the CIO/CISO.	6	(Bailey et al. 2014) (Bailey et al. 2020) (CII 2016; Higgs et al. 2016) (Liu et al. 2020) (Nolan and McFarlan 2005) (Olyaei et al. 2021)
3.	Reporting	M	The coverage includes use of items such as, security lifecycle, metrics based on COBIT, and high-level outline on the importance of lead indicators. Very limited literature providing examples, or generic reporting frameworks.	8	(AICPA 2018) (Banker and Feng 2019) (Cheong et al. 2021) (Lennon 2003) (Mandy et al. 2021) (Payne 2006) (Proctor 2021b) (Scholtz 2021)
4.	Assets	L	Some coverage of the need to classify which processes, information and systems need to be protected so that there is a fit-for-purpose approach to cybersecurity controls that brings ROI on investments in cybersecurity.	2	(Anderson et al. 2017) (Boehm et al. 2019)
5.	Culture	M	This is also inherent in Accountability, but these papers focus on people being the weakest link and enhancing security through gamification and application of the Protection Motivation Theory.	5	(Brown et al. 2017) (Donalds and Osei-Bryson 2020) (Rantos et al. 2012) (Schuetz et al. 2020) (Winnefeld Jr et al. 2015)
6.	Lexicon	L	Very limited coverage on the use of lexicon maps to assist non-technical and technical audiences to align on common terminology. The coverage includes the use of a series of reporting hierarchies.	2	(Savola 2007) (Savola 2008)

Table 5: Conceptual themes in final Candidate Papers

[2] High (H): >= 10 papers; Medium (M): 3-9 papers; Low (L): <3 papers. All out of a final pool of 54 candidate papers

Principles to guide cybersecurity governance for executives and board directors are found in literature across industry and academic sources. The World Economic Forum frames six principles that should be embedded to ensure a cyber-resilient organization (WEF 2021). This includes viewing cybersecurity as a business enabler, aligning the risk with business needs, and ensuring organizational design, including board governance, supports cybersecurity. Similarly, (CAQ 2018) and the material from the National Association of Company Directors (Leech and Hanlon 2017), outlines five principles boards should consider as they seek to enhance their capability in providing cybersecurity oversight. This includes a framework of questions that should be asked to provide assurance on cybersecurity matters. These questions are grouped to target the various actors involved in this process, including Auditors, Management and Directors. Furthermore (CII 2016) frames five questions to ask in order to understand the cybersecurity strategy, where weaknesses may exist, and then target investment in an informed manner.

Papers also have a consistent view on the *accountability* for cybersecurity sitting with the Board, but these fall short of explaining how this can be discharged with the right frameworks and tools. A range of sources frame the use of a Board sub-committee, (Nolan and McFarlan 2005), that has the skills and knowledge to drive cybersecurity as one way to build capability in the Board. Similarly (Bailey et al. 2020) argues the use of sub-committees can allow more time to delve into cybersecurity matters, than the board frequency itself. Further (Olyaei et al. 2021) also asserts that Boards see cybersecurity as top source of risk and as such should ensure they can exercise their accountability with the right skills themselves, and ensure reporting into committees engages in the right language. Another aspect of accountability from (Bailey et al. 2014) is that within management the CEO and other members of the senior leadership team are all accountable for security, and not just the CIO/CISO. This is reflective of elements of security, such as access control/logon and customer interactions, that sit across all parts of an organization. It goes on to expand that to fulfil this accountability leaders should focus on strategy, cross-business unit controls, user behavior and then sound governance and reporting. The organizational structures also play a key role in accountability and oversight as framed by (Liu et al. 2020). The authors state that centralized IT governance with a framework of indicators and metrics for reporting, gives a better outcome for reducing cybersecurity risk. Decentralized governance or a structure distributed across multiple divisions introduces variability in cybersecurity maturity, with additional cost and complexity.

Clarity on the nature of *reporting* required to enable board accountability to be fulfilled is limited. From an Audit perspective, (AICPA 2018) outlines a high level reporting framework that provides insights 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 also carries some importance in (Cheong et al. 2021) which outlines a way to report to regulators such as SEC, through disclosure reporting from management to Boards. These and similar references provide a high-level view of the nature of reporting frameworks, however they lack guidance across the whole security lifecycle, and also are limited in not outlining the data that should be requested, beyond that which frames the volume, velocity and severity of attacks on the perimeter network. 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 2021a). Gartner (Scholtz 2021) also states that security presentations and reports do not resonate with senior leaders and the Board and are rarely aligned to business drivers; in fact security is seen as a necessary evil rather than a business investment. Some literature, (Payne 2006), does frame basic attributes of security metrics, including some of the characteristics that are desirable for metrics, e.g. SMART – Specific, Measurable, Attainable, Repeatable and Time-dependent. Similarly, Gartner (Mandy et al. 2021) outlines an approach based on the CARE framework which requires metrics to be Consistent, Adequate, Reasonable and Effective.

In regards to *assets* that need protecting, there appears to be a one size fits all across all parts of the organization in terms of the approach to cybersecurity standards and reporting. This is framed in detail by (Boehm et al. 2019) which states that it is important to start with a focus on identifying and agreeing the assets that require protection. The assets can include business processes, systems enabling them, or even specific data sets. It is argued that such an approach is risk-based, and allows governance of cybersecurity in a more cost-effective manner. This concept in industry is termed as identifying the "crown jewels" to be protected, and then ensuring this scope gets the management attention ahead of other areas. Literature is limited in such guidance, including the steps and approach to identify these in context of cybersecurity, and the inevitable set of interconnected processes and systems in today's digital landscape.

The focus on *culture* is an important dimension that is articulated by a range of papers including (Rantos et al. 2012) who asserts that measurement of security awareness should be beyond purely completion of training with embedded quizzes. It frames a way of measuring the effectiveness of such programs through ongoing regular engagement given people are often seen as the weakest link in security. In addition (Winnefeld Jr et al. 2015) frames a similar approach to increase the effectiveness of culture initiatives. Some interesting insights are presented by (Donalds and Osei-Bryson 2020) in terms of stating that different leadership styles impact the security compliance and culture in a positive or negative way. Limited literature frames indicators of good cybersecurity culture, and 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) asserts that that elements of the Protection Motivation Theory could guide establishment of focus on the culture that is grounded on personal motivations.

Lexicon that is used in the boardroom is vastly different from the terminology of cybersecurity as used by those that implement security in a technical sense. As framed in Figure 1, the use of a common lexicon framework is key to enabling better understanding between those that govern cybersecurity from a leadership perspective and those responsible for technical implementation downstream. Whilst in industry, a number of business glossaries are available and published, literature is limited in this domain. Papers by (Savola 2007; Savola 2008) and (Kormos et al. 1999) frame a series of hierarchy / tree structures that outline taxonomy that enables non-technical audiences to define cybersecurity coverage (in context of metrics) for business-level security, information security, and those for products and services. However, a mapping to terminology (that is more prevalent amongst technical audiences) for two-way translation is lacking, and more recent research in this is absent. This impacts the effectiveness of reporting of cybersecurity into the Board when there is a limited understanding of the terminology in what is a complex technical topic.

The systematic literature review confirmed that cybersecurity is seen as an important matter for boards, and that the focus and coverage of literature at a principle level for this audience is strong. However as seen through the review of papers, literature is limited in the area of providing a generic framework that can be used to assist in terminology, frameworks and metrics to guide the expectations and set the tone from the Board in a data-driven manner. Prior literature on how to define meaningful and useful cybersecurity metrics can be extended to develop a framework of these. Furthermore, the wider cybersecurity definition and the concepts framed in Figure 2 (Concepts in Cybersecurity Definition) can be used ensure coverage of metrics is broad; and importantly focuses on both the technical and non-technical dimensions to protect organizations.

Contribution

The research conducted in this SLR demonstrates a gap in metrics and lexicon available for the senior executive and board director audience.

Whilst some forms of lexicon maps exist in a few papers, these require extension to the full breadth of concepts in the cybersecurity definitions framed in Figure 2. This would enable a more holistic understanding of cybersecurity by this stakeholder group.

Further, a set of metrics that are tangible and meaningful in measuring the cybersecurity risk profile by the stakeholder group are lacking. The research conducted to-date has identified good practices for defining tangible metrics, including the SMART framework (Payne 2006), and the CARE framework (Mandy et al. 2021). Such frameworks will be valuable to apply in the formulation of foundational metrics that can be used by senior executives and directors. Theories have been identified to guide future research. This includes Kernel theory to guide the formulation executive information system of data metrics, Common Ground theory to guide framing of lexicon, and Rational Choice theory to inform and validate appropriate metrics. The application of these theories to the required research is depicted in Figure 7.

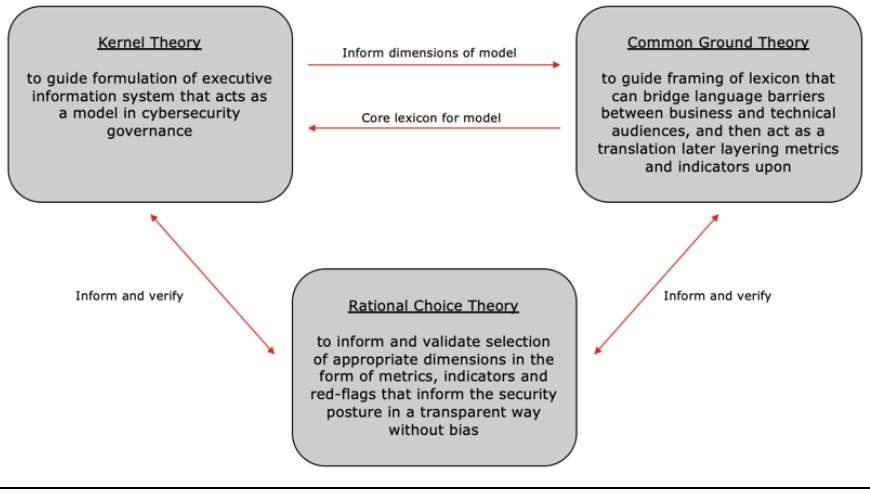

Figure 6: Guiding Theories in Research Design

It is expected that as the research progresses, further feedback on these theories (as it relates to such research problems) is expected. Furthermore, the contribution of this research will be to address literature gaps seen in this work to date for senior executives and board directors. This will provide a foundation for ongoing research, theoretical development and extension. The significance and contribution would extend to industry and practice (knowledge, literature and confidence amongst corporate/shareholder stakeholders) as well as to society (improve communications and trust through standard data driven cybersecurity metrics). This value of this contribution will address a real industry challenge for senior executives and board directors, in what is becoming a critical capability underpinning online digital services.

Conclusion

Cybersecurity governance is a mainstream challenge that requires ongoing targeted research and support from the academic world. In addition, such efforts need to work collectively with industry and government to understand the challenges faced in organizations when governing cybersecurity. This collaborative approach will assist in advancing the approach to governing what is a complex and ever-changing field.

Whilst senior executives and board directors are ultimately accountable for governing the security posture of their organizations, they are not provided with an industry standard data-driven model to help them.

In context of the research question, the findings have shown that the artefacts available for senior executives and board directors are limited. Further research is required into this area to formulate models that can be applied in a tangible manner. Such models would focus on metrics with clear business lexicon, and be data-driven to measure and improve the cybersecurity in organizations ongoing.

It is expected that by offering this stakeholder group more know-how and techniques on measuring the posture of cybersecurity, it will better enable them to drive improvement of cybersecurity risk through adage of 'what gets measured, gets managed'. This model should offer a foundation for improvement and extension, and be technology agnostic and enable ongoing evolution with industry change.

Acknowledgements

The Australian Government Research Training Program Scholarship for its support of this research.

Dr. Asif Gill, Associate Professor & Director of DigiSAS Labs at the UTS School of Computer Science for his guidance and constructive review of the paper.

References

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

AEMO. 2019. "Australian Energy Sector Cyber Security Framework (Aescsf)." from https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources

AICD. 2022. "Cybersecurity - Are You Taking the Necessary Steps and Measures to Reduce Your Exposure." from https://aicd.companydirectors.com.au/global/taxonomydetail?tax=Cybersecurity

AICPA. 2018. "Soc for Cybersecurity: A Backgrounder." American Institute of Certified Public Accountants

AlGhamdi, S., Win, K. T., and Vlahu-Gjorgievska, E. 2020. "Information Security Governance Challenges and Critical Success Factors: Systematic Review," *Computers and Security* (99).

Allen, J. 2005. "Governing for Enterprise Security," Carnegie Mellon Software Engineering Institute.

Anderson, C., Baskerville, R. L., and 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), pp. 1082-1112.

APRA. 2010. "Cps 231 Outsourcing." APRA.

APRA. 2019. "Cps 234 Information Security." APRA.

ASD. 2020. "Essential Eight." Australian Signals Directorate.

ASIC. 2015. "Cyber Resilience: Health Check." ASIC.

ASIC. 2019. "Cyber Resilience of Firms in Australia's Financial Markets: 2018–19." from 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. "Asic Commences Proceedings against Ri Advice Group Pty Ltd for Alleged Failure to Have Adequate Cyber Security Systems." from 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/

ASX/ASIC. 2017. "Asx 100 Cyber Health Check Report."

AustCyber. 2021. "Australian Cyber Security Growth Network." from https://www.austcyber.com/about-us

Azmi, R., Tibben, W., and Win, K. T. 2018. "Review of Cybersecurity Frameworks: Context and Shared Concepts," *Journal of cyber policy* (3:2), pp. 258-283.

Bailey, T., Banerjee, S., Feeney, C., and Hogsett, H. 2020. "Cybersecurity: Emerging Challenges and Solutions for the Boards of Financial- Services Companies," McKinsey.

Bailey, T., Kaplan, J., and Rezek, C. 2014. "Why Senior Leaders Are the Front Line against Cyberattacks," McKinsey.

Banker, R. D., and Feng, C. 2019. "The Impact of Information Security Breach Incidents on Cio Turnover," *Journal of Information Systems* (33:3), pp. 309-329.

Baxter, R. J., Holderness Jr, D. K., and Wood, D. A. 2016. "Applying Basic Gamification Techniques to It Compliance Training: Evidence from the Lab and Field," *Journal of Information Systems* (30:3), pp. 119-133.

Boehm, J., Curcio, N., Merrath, P., Shenton, L., and Stähle, T. 2019. "The Risk-Based Approach to Cybersecurity," McKinsey.

Brown, J. O., Marcum, J. A., and Stuebs Jr, M. T. 2017. "Professional Virtue Reinforcements: A Necessary Complement to Technological and Policy Reforms," *Journal of Information Systems* (31:2), pp. 5-23.

Bruin, R. D., and Solms, S. H. v. 2016. "Cybersecurity Governance: How Can We Measure It?," *2016 IST-Africa Week Conference*, pp. 1-9.

Cains, M. G., Flora, L., Taber, D., King, Z., and Henshel, D. S. 2021. "Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context Using Expert Elicitation," *Risk Analysis*).

CAQ. 2018. "Cybersecurity Risk Management Oversight." Center for Audit Quality

Carcary, M., Renaud, K., McLaughlin, S., and Brien, C. O. 2016. "A Framework for Information Security Governance and Management," *IT Professional* (18:2), pp. 22-30.

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

Cheong, A., Yoon, K., Cho, S., and No, W. G. 2021. "Classifying the Contents of Cybersecurity Risk Disclosure through Textual Analysis and Factor Analysis," *Journal of Information Systems* (35:2), pp. 179-194.

CII. 2016. "Prioritizing Cybersecurity," Council of Institutional Investors.
CISA. 2019. "What Is Cybersecurity?", from https://us-cert.cisa.gov/ncas/tips/ST04-001
CISCO. 2021. "What Is Cybersecurity?", from https://www.cisco.com/c/en_au/products/security/what-is-cybersecurity.html
Clinton, L., Higgins, J., and van der Oord, F. 2020. "Cybersecurity Risk Management Oversight," National Association of Corporate Directors and the Internet Security Alliance.
Craigen, D., Diakun-Thibault, N., and Purse, R. 2014. "Defining Cybersecurity," *Technology Innovation Management Review* (4:10).
Cram, W. A., Proudfoot, J. G., and D'Arcy, J. 2021. "When Enough Is Enough: Investigating the Antecedents and Consequences of Information Security Fatigue," *Information Systems Journal* (31:4), pp. 521-549.
Donalds, C., and Osei-Bryson, K.-M. 2020. "Cybersecurity Compliance Behavior: Exploring the Influences of Individual Decision Style and Other Antecedents," *International Journal of Information Management* (51), p. 102056.
Fischer, C., Winter, R., and Wortmann, F. 2010. "Design Theory," *Business & Information Systems Engineering* (2:6), pp. 387-390.
Gielens, K., and Steenkamp, J.-B. E. M. 2019. "Branding in the Era of Digital (Dis)Intermediation," *International Journal of Research in Marketing* (36:3), pp. 367-384.
Guthrie, C., Fosso-Wamba, S., and 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), p. 102570.
Haislip, J., Lim, J.-H., and Pinsker, R. 2021. "The Impact of Executives' It Expertise on Reported Data Security Breaches," *Information Systems Research* (32:2), pp. 318-334.
Harmer, G. 2013. *Governance of Enterprise It Based on Cobit 5 : A Management Guide*, (1st edition ed.). Cambridgeshire, [England: IT Governance Publishing.
Higgs, J. L., Pinsker, R. E., Smith, T. J., and Young, G. R. 2016. "The Relationship between Board-Level Technology Committees and Reported Security Breaches," *Journal of Information Systems* (30:3), pp. 79-98.
Iden, J., and Eikebrokk, T. R. 2013. "Implementing It Service Management: A Systematic Literature Review," *International Journal of Information Management* (33:3), pp. 512-523.
ISO. 2013a. "Iso/Iec 27001 - Requirements for Continually Improving an Information Security Management System." ISO.
ISO. 2013b. "Iso/Iec 27002 - Selection, Implementation and Management of Controls ". ISO.
ISO. 2018. "Iso/Iec 27000 - Overview of Information Security Management Systems (Isms)." ISO.
Kappelman, L., Johnson, V. L., Maurer, C., Guerra, K., McLean, E., Torres, R., Snyder, M., and Kim, K. 2020. "The 2019 Sim It Issues and Trends Study," *MIS Quarterly Executive* (19:1), pp. 69-104.
Kormos, C., POC, L. A. G., Givans, N., and Bartol, N. 1999. "Using Security Metrics to Assess Risk Management Capabilities," *National Information Systems Security Conference*.
Lee, C. H., Geng, X., and Raghunathan, S. 2016. "Mandatory Standards and Organizational Information Security," *Information Systems Research* (27:1), pp. 70-86.
Leech, T. J., and Hanlon, L. C. 2017. *Board Cyber Risk Oversight*. Hoboken, NJ, USA: John Wiley & Sons, Inc.
Lennon, E. 2003. "It Security Metrics," NIST.
Li, L., He, W., Xu, L., Ash, I., Anwar, M., and Yuan, X. 2019. "Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior," *International Journal of Information Management* (45), pp. 13-24.
Liu, C.-W., Huang, P., and 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), pp. 758-787.
Mandy, C., Olyaei, S., and Proctor, P. 2021. "Metrics to Prove You Care About Cybersecurity," Gartner.
McLaughlin, M.-D., and Gogan, J. 2018. "Challenges and Best Practices in Information Security Management," *MIS Quarterly Executive* (17:3), pp. 237-262.
Merriam, W. 2013. *Webster's American English Dictionary*. Federal Street Press.
NIST. 2018. "Framework for Improving Critical Infrastructure Cybersecurity." NIST.
NIST. 2019. "Computer Security Resource Center (Csrc)." *NISTIR 7298 Rev. 3*, from https://csrc.nist.gov/glossary/term/Cyber_Security
Nolan, R., and McFarlan, F. W. 2005. "Information Technology and the Board of Directors," *Harvard business review* (83:10), pp. 96-157.

Okoli, C., and Schabram, K. 2010. "A Guide to Conducting a Systematic Literature Review of Information Systems Research,").
Olyaei, S., Thielemann, K., Addiscott, R., and Pratap, K. 2021. "Predicts 2021: Cybersecurity Program Management and It Risk Management," Gartner.
OpenGroup. 2017. "Open Information Security Management Maturity Model (O-Ism3), Version 2.0." The Open Group.
Payne, S. 2006. "A Guide to Security Metrics," SANS Institute.
PCI. 2018. "Data Security Council - Requirements and Security Assessment Procedures." Payments Industry Council
Pienta, D., Thatcher, J. B., and Johnston, A. 2020. "Protecting a Whale in a Sea of Phish," *Journal of Information Technology* (35:3), pp. 214-231.
Proctor, P. 2021a. "An Outcome-Driven Approach to Cybersecurity Improves Executive Decision Making," Gartner.
Proctor, P. 2021b. "Outcome-Driven Metrics for Cybersecurity in the Digital Era," Gartner.
Rantos, K., Fysarakis, K., and Manifavas, C. 2012. "How Effective Is Your Security Awareness Program? An Evaluation Methodology," *Information security journal.* (21:6), pp. 328-345.
Rout, D. 2015. "Developing a Common Understanding of Cybersecurity," *ISACA JOURNAL* (Volume 6).
Savola, R. 2007. "Towards a Taxonomy for Information Security Metrics," in: *Proceedings of the 2007 ACM workshop on Quality of protection*. Alexandria, Virginia, USA: Association for Computing Machinery, pp. 28–30.
Savola, R. 2008. "A Novel Security Metrics Taxonomy for R&D Organisations," *ISSA*, pp. 379-390.
Scholtz, T. 2021. "How to Communicate the Value of Information Security in Business Terms," Gartner.
Schuetz, S. W., Benjamin Lowry, P., Pienta, D. A., and Bennett Thatcher, J. 2020. "The Effectiveness of Abstract Versus Concrete Fear Appeals in Information Security," *Journal of Management Information Systems* (37:3), pp. 723-757.
Smith, P. 2020. "Hacked Again: Toll Group Systems Hit by Fresh Ransomware Attack." Retrieved 5 May 2020, from https://www.afr.com/technology/hacked-again-toll-group-systems-hit-by-fresh-ransomware-attack-20200505-p54q19
Stevenson, A. 2010. *Oxford Dictionary of English*, (3rd ed. / edited by Angus Stevenson. ed.). Oxford: Oxford University Press.
SWIFT. 2020. "Swift Customer Security Controls Framework (Cscf) ". SWIFT.
von Solms, R., and van Niekerk, J. 2013. "From Information Security to Cyber Security," *Computers & Security* (38), pp. 97-102.
Walls, A., Perkins, E., and Weiss, J. 2014. "Definition: Cybersecurity," Gartner.
Walton, S., Wheeler, P. R., Zhang, Y., and Zhao, X. 2021. "An Integrative Review and Analysis of Cybersecurity Research: Current State and Future Directions," *Journal of Information Systems* (35:1), pp. 155-186.
Ward, M. M., Max. 2021. "Effects on Cyber Attack on Nine Set to Linger." Retrieved 28 Mar, 2021, from https://www.afr.com/companies/media-and-marketing/suspected-cyberattack-hits-nine-20210328-p57epg
Warner, M. 2012. "Cybersecurity: A Pre-History," *Intelligence and National Security* (27:5), pp. 781-799.
WEF. 2021. "Principles for Board Governance of Cyber Risk," World Economic Forum.
Wilkes, G. A., and Krebs, W. A. 1995. *Collins Concise Dictionary*, (3rd ed. / special Australian consultants G.A. Wilkes, W.A. Krebs. ed.). Sydney: HarperCollins.
Winnefeld Jr, J. A. S., Kirchhoff, C., and Upton, D. M. 2015. "Cybersecurity's Human Factor: Lessons from the Pentagon " *Harvard Business Review HBR* (93:9), pp. 86-17.