Leadership in Organisational Cyber Security

by

GEORGIA PSAROULIS

AdvDip. Accounting (TAFE NSW)

B. Business Administration (Acc and IS) (Western Sydney University)

M. Business Administration (Sydney Graduate School of Management)

GradCert. Sc (Computer Forensics) (University of South Australia)

Submitted in total fulfilment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

in

Business School, Faculty of The Professions University of Adelaide

Date Submitted: February 2022

ABSTRACT

Globally, most organisations are powerless to protect their information assets against the constant threat of hostile intruders, and leaders are uncomfortable with the potential threat and disruption to the deep-seated norms, patterns, and systems in their organisational setting. Yet little research exists on Leadership in Cyber security and existing cyber research is splintered across literature specific to individual disciplines that are only component domains of the broader cyber security multidiscipline.

This study identifies and addresses “the role of strategic leadership in the complex issue of organisational cyber security”. This thesis argues that cyber security is a complex multidisciplinary leadership issue that must be – but usually is not – addressed systemically. This premise was formulated during employment in the cyber domain and my and colleagues’ experiences provided empirical drivers to investigate this phenomenon.

Experience and anecdotal evidence indicated absence of corporate governance in organisational cyber security and ill-defined cyber-OAR (Ownership, Accountability and Responsibility). Chief Information Security Officers (CISOs) lack requisite status, and despite multiple stakeholders and government publications, most executives remain cyber-unaware and have no relationship with the CISO – if they have a CISO at all. Yet these vital issues remain unaddressed in academic publications.

In late 2017, almost no literature existed on the topic and the focus issues were largely unrecognised and ignored. In ensuing years, some recognition and changes have emerged. Promising regulations have been introduced, previously unrecognised aspects researched and published, and visionary cyber leadership has emerged – which might suppose the research topic to be obsolete and unnecessary. But in 2022, the situation is unresolved and despite visionaries, and increased government spending and awareness-building efforts, organisational cyber security is still not understood or practised by most executives.

As an academic discipline and organisational practice, cyber security is still in its infancy. An emerging stream of research reveals multiple issues, including fragmentation across multiple academic and practitioner disciplines. Focus has typically remained on technical issues and challenges as computer science and information technology disciplines contribute the majority of published cyber security research, and only scattered articles address non-technology aspects of cyber security. Despite burgeoning interest in the ‘human aspects of cyber security’, when first scoped – with one exception – no research addressed cyber corporate leadership and/or cyber governance ecosystems. This accumulation of worrisome issues is increasingly critical for organisational survival and wellbeing and is substantive evidence of the need for research to address organisational cyber security and leadership.

Planned as a thesis-by-publication, this research was purposefully designed as a three-phase study spanning five–six years. An exploratory study, the approach

had to be qualitative and emergent. As an infant multidisciplinary domain, the first phase needed to be a scoping review to explore and compare literature across the principal sub-domains. Research commenced with exploring cyber security as a strategic, corporate governance issue that is complex, multidisciplinary, and currently fragmented. Analysis of the scoping review findings confirmed the original premise sufficiently to require a targeted literature review and permitted early conceptual models to be developed, graphically depicting the issues and their interrelationships, and to shape potential solutions and an aspirational future state of organisational cyber security and leadership.

The Phase 2 targeted review led to the design of an empirical investigation. Guided by review findings, participants were selected, and questions designed. Interviews were conducted with 31 participants from 24 organisations from the Finance sector, following guidelines approved in HREC (**H-2019-127**). Analysis was primarily conducted using a series of coding passes; constant comparison, pattern and theme, and reduction of the multiple produced theme-codes to a few tightly focussed supra-codes. Graphic analysis was used throughout, creating a series of models to illustrate and synthesise findings, and develop conceptual frameworks. This coding method of analysis was also used for the literature reviews.

Stakeholder theory was the primary filter for all analysis, selected due to the original premise that organisational cyber security is multidisciplinary but siloed and fragmented in academia and praxis. In Phase 3, the principal focus was deeper exploration through theoretical lenses and to develop new theory.

Stakeholder theory remained the foundation, but all findings were revisited using a theoretical filter of Triple-loop learning.

Papers for each of the three phases have been submitted to a leading journal. The body of this thesis is comprised of these papers in entirety, preceded and followed by a whole-of-work introduction and conclusion. The three papers are co-authored but all the initial foundations, including premises, questions, research objectives, interviews, analysis, and models are my original work. Therefore, from Chapter 4 onwards, I refer to the researcher/ author in the plural, acknowledging the contribution of my supervisor/co-author, Dr Cate Jerram.

Findings, conclusions, and recommendations are documented in the three abstracts, but briefly recapitulated here. Phase 1 concluded that traditional silos must be bridged or discarded, and a new common lexicon developed. Cyber security lexicons and approaches must align with corporate strategy. Organisational executives must acknowledge and take ownership, accountability, and responsibility for their organisation's cyber security, and immediately address the role, status, and budget of the CISO.

Phase 2, building from Phase 1, revealed that key mechanisms of corporate governance must promote a shared stewardship approach. The CEO and the CISO must work together and resolve cyber-OAR issues, and the corporate governance system and mechanisms need to simultaneously change and align with the CEO-CISO-OAR relationship. Any aspirational future state cyber security must be embedded in a cyber corporate governance ecosystem. Phase 3

concluded our study with theoretical development and found Triple-loop learning approaches can reinvent and transform organisational cyber security.

Clear and coherent cyber security must be directed by strategic leadership and the business and cyber ecosystems must be integrated and intrinsically link. As evidenced by the dearth of quality literature discussing the issues addressed here, few resources are available in this domain and all work in this thesis is original, except where referenced.

This study makes three major contributions to theory and practice. Firstly, organisational safety and wellbeing requires corporate cyber governance that is led by the Executive. Secondly, it is imperative that the CISO be a strategic trusted advisor in cyber corporate governance, security, and resilience. Thirdly, any progress in advancing organisational cyber security is dependent on eliminating disciplinary fragmentation based in academic and professional silos, instead building cooperation and co-opetition, collaboration, and eventually a coherent, systemic multidiscipline. Finally, models are provided to illustrate these three major contributions and subsidiary contributions, culminating in the proffered concept of an aspirational future state of what we refer to as – ‘cyber corporate governance ecosystem’.

This research has produced contributions of value to research and praxis, and frequently to both. The contributions have significant implications that should affect current practice in organisational cyber security and leadership and pave the way for important new fields of research. Significant secondary contributions

to practice include the recommendation that silos be discarded to enable a strong and holistic multidiscipline of cyber security.

The first implication is that disciplines, professional bodies, and cyber educators (and all extended enterprise) need to strengthen collaboration and establish synergies. Government and quasi-governmental regulators play a vital lead role in cyber security but need to improve dissemination for wider uptake. Organisations, however, need both to become more aware and adoptive of regulations and government provisions, but must improve their ability to adapt any such adoptions to ensure appropriate cultural alignment. Principally, however, Executives must lead and coordinate, determine priorities, and break down barriers to meet organisational need, starting with recognition of the strategic value of cyber security and trusting the CISO as a vital strategic advisor.

This research was conducted part-time over six–years in a rapidly changing digital environment that preceded and included the COVID-19 pandemic and its aftermath (and ongoing ‘new normal’), which has inevitably affected the results. This is, though timely, a date-specific limitation. The span of time also saw changes eventuating in the cyber security domain that is the focus of the study. Nevertheless, though the constantly changing cyber landscape has been an impediment to conducting the research, effects on results, conclusions and recommendations have been minimised as much as possible.

Primary research limitations are those inherent to qualitative approaches. Empirical investigation through semi-structured interviews provided depth but prohibited large numbers for generalisability. Transferability to other sectors is a

possibility, but the original field of enquiry was restricted to the Finance sector. Although an investigation into leadership in organisational cyber security, few participants were themselves CEOs or organisational Board members. Further research is needed across different industry-sectors, qualitative research directly engaging with Executive and Board members is needed, and sufficient explorative studies are required to eventually enable broader, generalisable studies.

DECLARATION

This work contains no material which has been accepted for the award of any other degree or diploma in any university or other tertiary institution to **Georgia Psaroulis** and to best of my knowledge and belief, contains no material previously published or written by another person, except where due reference has been made in the text.

In addition, I certify that no part of this work will, in the future, be used in a submission in my name, for any other degree or diploma in any university or other tertiary institution without the prior approval of the University of Adelaide and where applicable, any partner institution responsible for the joint-award of this degree. The author acknowledges that copyright of published works contained within the thesis resides with the copyright holder(s) of those works.

I also give permission for the digital version of my thesis to be made available on the web, via the University's digital research repository, the Library Search and also through web search engines, unless permission has been granted by the University to restrict access for a period of time. I acknowledge the support I have received for my research through the provision of an Australian Government Research Training Program Scholarship.

Signed: Date: 4/02/2022

ACKNOWLEDGEMENT

First and foremost, I would like to acknowledge my mentor and principal supervisor, Dr Cate Jerram, for her unwavering support, recommendations and steadfast reinforcement that guided my academic journey. Also, a special mention for working closely together and co-authoring the three research articles (published forthcoming). Thank you

This has been a long and challenging processes but an accomplishment so worth it.

DEDICATION

To my husband Spiros. Thank you for standing by me.

My sons Jayden and Aidan. Thanks for your constant support and encouragement.

.

RESEARCH PROFILE

Psaroulis, G., Jerram, C., (forthcoming) “The ‘Corporate Governance Paradox’” that allows silos and fragmentation to defeat organisational cyber resilience, (submitted to Journal of Strategic Information Systems).

Psaroulis, G., Jerram, C., (forthcoming) “Which comes first? The CEO and CISO roles and responsibility? or the principles of OAR (ownership, accountability, and responsibility)? (submitted to Journal of Strategic Information Systems).

Psaroulis, G., Jerram, C., (forthcoming) “The aspirational future state of cyber security: A cyber corporate governance ecosystem”, (submitted to Journal of Strategic Information Systems).

TABLE OF CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

CHAPTER 1: INTRODUCTION

1.1 Thesis outline

Cyber threats and sophisticated, mass-scale cyber-attacks have increased in frequency, scale, and sophistication over the last few years, “potentially crippling core business functions” (ACSC 2020, p. 10) and causing substantial harm to organisations in every sector across the globe. The exponential level of cyber risk and damaging consequences of successful cyber-attacks mean that cyber security is now widely recognised as critical to organisational survival. This acknowledgement clearly places cyber risk in the domain of risk management, organisational leadership, and strategic planning.

Cyber security has become a ‘hot topic’. Yet despite rapid growth in literature on the subject, research on the role of leaders in organisational cyber security is in its infancy (Hasib 2015; Tisdale 2016). Apart from contributions in top-quintile journals from high profile thought leaders and experts, integrating cyber security into corporate governance has made little progress. Cyber security is often ‘unwelcome’ in organisations where leaders are uncomfortable with its threat to disrupt the deeply embedded norms, patterns and systems existing in the organisational setting.

Over recent years, we have seen an increased focus on cyber security in organisations and increased spending on aspects of cyber security. Yet even state-of-the-art cyber security offerings do not necessarily yield adequate protection of the organisation’s ‘crown jewels’ or critical capabilities. Furthermore,

in many cases, organisations do not yet understand the need to extend beyond cyber protection and defence to organisational resilience – the ability to survive after a successful cyber-attack.

Cybercrime was defined in 2015 by IBM Chairman Rometty, as “the greatest threat to every profession, every industry, and every company in the world” (Morgan 2015, p. 11). Despite the growing focus on cyber security by many experts and cyber-thought leaders across academia, government and regulatory bodies in recent years, Rometty’s statement remains true. Since 2019, the societal changes created by COVID-19 have, in fact, stimulated criminal cyber activity and raised the risk level.

“2021 has been a banner year for cybercriminals” (Carlson 2021, p. 11), and according to the ACSC Cyber Threat Report 2020-21, a cyber-attack is now reported every 8 minutes in Australia alone (ACSC 2021). “But there’s a problem: in many cases, increased spending on cybersecurity in recent years hasn’t resulted in better protection against hackers" (Rosenbaum 2021, p. 2). This is not surprising as:

> PwC’s 2022 Global Digital Trust Insights Survey (GDTI) shows that more than half of Australian organisations have less than a thorough understanding of the risk of data breaches through third-parties, while nearly one-fifth have little or no understanding at all of these risks (Caisley 2021, p. 11).

One element of the ‘little or no understanding at all of these risks’ is that leaders with a comprehensive understanding of ‘normal’ assets, are often unaware of information assets, and have little concept of the crown jewels or the value of data. Over the last four decades, the role of ‘data’ and its value has evolved to become a key strategic resource that deserves to be managed and protected as professionally and aggressively as other company assets. An April 2016 study found that:

> 91% of Board Members at the most vulnerable companies can’t interpret a cybersecurity report... 40% said they feel no responsibility for the consequences of being hacked (Tanium in partnership with NASDAQ - UPGUARD 2016).

Years later, not much has changed according to the latest data available. Since 2016, many organisations have increased spending on cyber security (although many purchases don’t get deployed), but this does not lead to better defence (Rosenbaum 2021, p. 22). This is possibly because more than half of the executives, still do not fully understand the nuances of the cyber risk posed to their organisation or the myriad substandard cyber reports they receive (Caisley 2021; PwC 2021).

The accepted “relaxed, anxious, ignorant” attitudes by the Executive (Towers-Clark 2018, p. 11) is problematic as they “ultimately shoulder the blame” (MIT Technology Review 2016, p. 11). According to the 2022 Gartner Board of Directors Survey, "Eighty-eight per cent of Boards of Directors (BoDs) now viewed cyber security as a business risk” (Gartner 2021, p. 11). Hence “it's time

for these executives outside IT to take responsibility for business decisions that affect enterprise security" (Gartner 2021, p. 11).

A developmental approach was taken for this PhD research to investigate the complex and largely unexplored issue of strategic leadership in organisational cyber security. Only recently has published research alleged that "Cybersecurity (CS) is a leadership, not a technical issue", (Tisdale 2016, p. 44) and categorised cyber security leadership as "a business discipline" (Hasib 2015, p. 44) that needs to "start with the highest executive level of an organization" (Hasib 2015, p. 55). Despite this recognition, little has been done in research or practice to challenge or substantiate and address these allegations.

1.1.1 Thesis-by-publication

This is a thesis-by-publication that includes three papers (submitted to leading journals), each reporting on a major phase of the study. Phase 1 (Paper 1) examines the current landscape of organisational cyber security through an extensive multi-disciplinary scoping review.

> Psaroulis, G., Jerram, C., (forthcoming) "The 'Corporate Governance Paradox'" that allows silos and fragmentation to defeat organisational cyber resilience, (submitted to Journal of Strategic Information Systems).

Phase 2 (Paper 2), built on Phase 1, commencing with a refined and focussed in-depth literature review followed by a qualitative empirical investigation.

> Psaroulis, G., Jerram, C., (forthcoming) "Which comes first? The CEO and CISO roles and responsibility? or the principles of OAR (ownership,

accountability, and responsibility)?" (submitted to Journal of Strategic Information Systems).

Phase 3 (Paper 3) synthesises the findings through theoretical lenses and develops models to illustrate major finding and conclusions.

Psaroulis, G., Jerram, C., (forthcoming) "Cyber corporate governance ecosystem – the aspirational future state", (submitted to Journal of Strategic Information Systems).

The structure of this thesis, therefore, is as follows:

This Introduction (Chapter 1) presents the context and drivers of the research study. Chapter 2 is a literature review of the complex systems issue of leadership and cyber security. Chapter 3 provides research methodology and methods for the three phases. Phases 1, 2, and 3 are then described respectively in Chapter 4, 5 and 6 presented as the stand-alone manuscripts submitted to journals. Finally, Chapter 7 provides a conclusion, recommendation, contribution to academia and practice, followed by the limitation and finally the implication for cyber stakeholders.

CHAPTER 2: LITERATURE REVIEW

2.1 Complex system issue: leadership, governance and cyber security

In the last decade, cyber security – recognised as operationally important and traditionally tightly linked to IT (Frauenstein & Von Solms 2014) – has emerged as strategically important. Strategic importance elevates cyber security from an IT issue for which the CIO and/or CISO could reasonably be held responsible, to a strategic – therefore corporate governance – issue, making it the responsibility of the Executive.

Even when recognised theoretically, this has not found its way into the practice of corporate governance. As was highlighted in the 2017–2019 *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry* that "if leadership is measured by impact" then this industry has changed forever (Knight 2018, p. 11) by the failures of leadership, governance, and accountability. Reflecting on this new paradigm, what became apparent was that senior management had under-supervised the firm's operations (Goyder 2002). To put it simply, leaders had evaded their responsibility by making someone else responsible and had kept immature governance protocols and sustained complex, under-developed and isolated information systems. However, this practice can no longer be excused for failing to manage risk, sustain performance and earn trust; nor can this overflow into cyber security (Linden & Staples 2018).

Notwithstanding the dramatic increase on research cyber security, the focus remained on technical issues and challenges. More recent research is emerging on human factors focused primarily on cyber security awareness, social engineering, human vulnerabilities, and similar. Yet, on the issue of 'leadership in cyber security', there is still a dearth of research or material. This was a primary driver for the research presented in this thesis.

A significant consequence of the failure to address cyber security as a strategic and systemic challenge needing to be addressed across the organisation's ecology is that cyber security is currently being approached in silos. The dominant silo is IT, but all departments affect and are affected by cyber security, making it an extremely multi-disciplinary issue. The multi-disciplinary fragmented silos add to the lack of strategic planning or overview which further inhibits effective cyber security measures. This concept was the second primary driver of this research.

The basic premise underlying this research is that cyber security is a complex leadership issue, with multiple critical facets that must be addressed systemically – in relation to one another and not as a singular and isolated domain. The primary premise driving this research is that cyber security is a complex leadership issue. These premises were formulated through a combination of experience and my early reading across multiple dimensions of the cyber domain. As described in the Methodology and Methods section, the premises were refined in several iterations to become the basis for a scoping review that became Paper 1, and the foundation, of this research.

In the course of identifying the driving issues and premises, I created a series of models to graphically depict the issues and their interrelationships. The resultant models are too complex (and 'messy') for publication in research journals but are provided in this thesis as necessary foundations for the subsequent research.

Here I present some of my original insight to the abovementioned premise, specifically asking why cyber security should be perceived as a leadership issue rather than a technology issue. I commenced with a series of mind maps capturing my understanding of the issues from my experience as a cyber professional in the finance sector and extensive preliminary reading. Mind map 1: leadership (Figure 2.1) visually presents what is needed of leadership, Mind map 2: cyber security (Figure 2.2) depicts essential aspects of organisational cyber security. With these initial mind maps capturing my understanding of the issues I was compelled to explore; I combined and refined the Mind map diagrams to a conceptual model.

Figure 2.1. Mind map 1: leadership

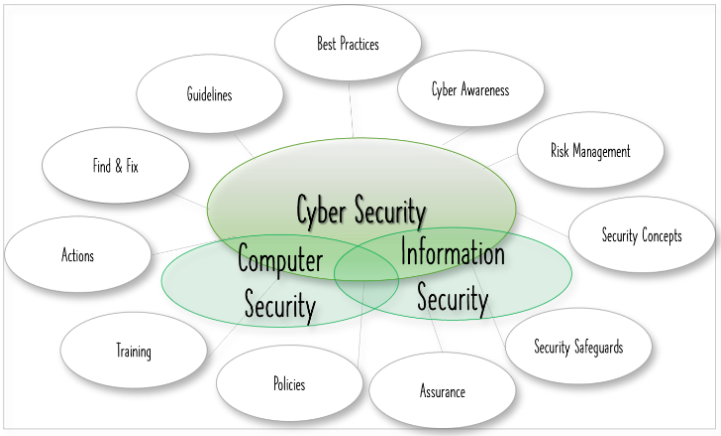

Figure 2.2. Mind map 2: cyber security

To reduce the chaos and complexity identified in the mind map diagrams, I simplified the conceptual model, breaking it into a three-part series. Figure 2.3 summarises core aspects that literature claims are central to leadership in an organisation. Figure 2.4 outlines the principal components of the cyber security domain. The contents of Figure 2.3 and Figure 2.4 are then 'assumed' in Figure 2.5, which depicts my underlying thesis – that leadership should undertake core responsibility for the cyber security of an organisation.

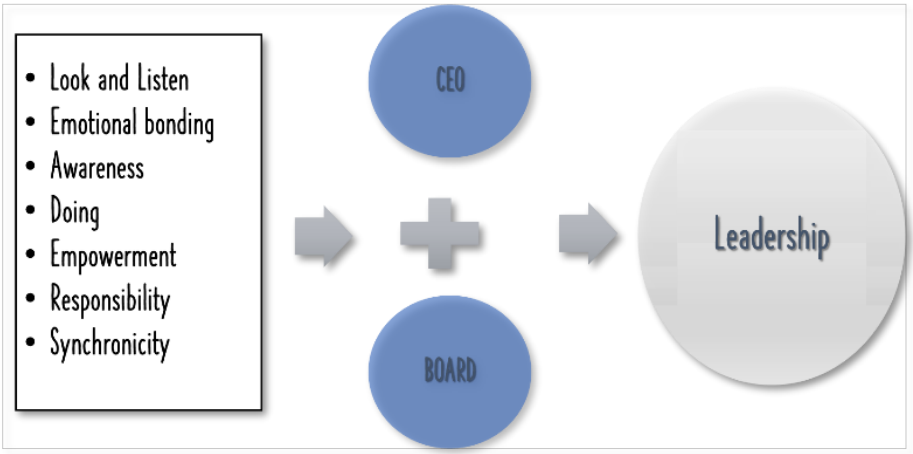

Figure 2.3. The complex systems issue of leadership

The explanation follows the diagram presented in Figure 2.3. Leadership requires many skills including, (1) Look and listen; (2) Emotional bonding; (3) Awareness; (4) Doing; (5) Empowerment; (6) Responsibility; (7) Synchronicity (Meier 2011). “Leaders operate in the realms of bewildering uncertainty and staggering complexity” (Reed 2006, p. 10) – success only comes by looking at the big picture – “leaders must see what is actually happening over what they want to see happen”. (Reed 2006, p.13).

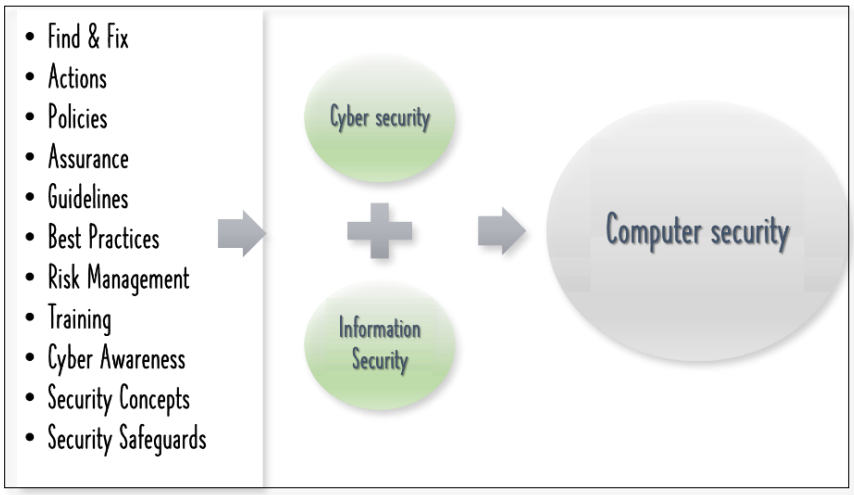

Figure 2.4. The complex systems issue of cyber security

The complex systems issue of cyber security by definition and in practice does not capture the interdisciplinary fields of Information Systems and Computer Security nor does it take into account the multi-layer elements and activities (detailed below) that are needed to act in concert to resolve the complex cyber security challenge (Craigen, Diakun-Thibault & Purse 2014). This is shown in Figure 2.4, ‘the complex systems issue of cyber security.

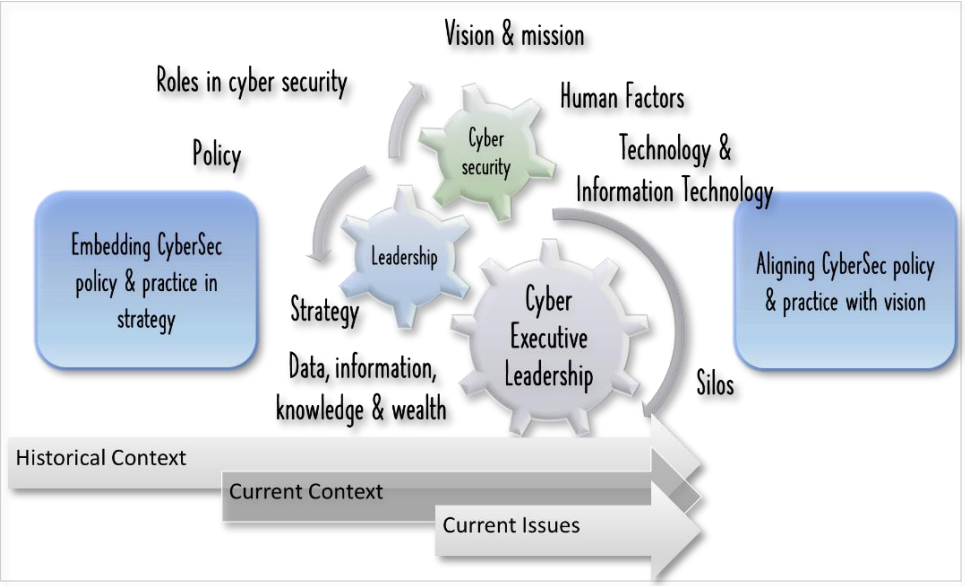

Figure 2.5. The complex systems issue of leadership and cyber security

The complex system model in Figure 2.5 presents the current struggle faced by many organisations in this perfect storm of cyber security (Reynolds & Tamburello 2016). Put simply, executives still do not understand it. The complex systems issue of the Leadership and cyber security (Figure 2.5) shows there is confusion, misinformation and at times disinformation that prevent the efforts to mitigate organisational cyber risk. The model highlights that cyber security needs be embedded in and aligned to the organisation's vision, mission, and strategic operations (namely corporate governance) for an organisation to be cyber safe and achieve resilience and move forward. This aspired state needs to be driven by the highest-level executives. Thus, the model depicts independent gears of cyber security and leadership that form the interrelated and interlocking components that turn the wheels (McKnight & Chervany 2006) of cyber security leadership.

In the remainder of this section, firstly, the definition of cyber security is discussed, and the definition ramifications are explored. Then I briefly examine the importance and value of data (and information) and why it has suddenly become so vital, exploitable, and vulnerable to theft, ransom, and misappropriation. Next, I focus on the current state of data and technology in cyber security, then survey recent history to examine how the current context emerged. This is followed by a summary of the more recently recognised issue of human factors in cyber security, and how this is perceived.

I then explore the interaction between leaders and the role and management of technology in organisations. I examine the parallel interaction between leaders and the organisation's data, information, and knowledge, with a specific focus on the consequent developments in the interaction between the role of leadership and cyber security.

This discussion will make clear that a constant, throughout all the topics under discussion, is that of silos – silos of information, silos of knowledge, and silos of responsibility. These silos are detrimental to the organisation, and, in particular, hamper the ability to make and keep an organisation cyber-secure. This discussion then leads to the issues at hand – the role of leadership in cyber security to ensure a holistic, rather than a siloed, approach. This issue requires use of a systems approach to adequately address the complexity.

I proceed to explore the interaction between leaders and the role and management of technology in organisations. I examine the parallel interaction between leaders and the organisation's data, information, and knowledge, with a

specific focus on the consequent developments in the interaction between the role of leadership and cyber security.

2.1.1 Definition of cyber security

The definition adopted for cyber security in this research is taken from the International Telecommunications Union (ITU) and states that cyber security touches several domains, and:

> 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 (2008, p. 22).

This description highlights that cyber security orchestration goes beyond merely protecting the organisation's information or information systems resources in cyberspace; it also needs to protect the person(s) using resources in a cyber environment (Von Solms & Van Niekerk 2013). These concepts identify the holistic and complex multi-disciplinary approach needed to support cyber security.

2.2 Current context: role of data and its value

The role of "data" and its value has evolved in organisations from the manual era, through to the technology revolution and now the cyber security epoch. Data has realistically been the cornerstone of organisations from the very beginning and is seen as a determinant factor that enables organisations to plan, control, operate,

make decisions, and drive business success. Nevertheless, its value has historically been taken for granted, and only recently been recognised and perceived as a vital and critical resource (Bhatt 2000a).

Interestingly, it is the threat of cyber-attack that has strengthened and more recently validated the value of “data”. Its newly understood value as mentioned in the Introduction and extended here is IBM Corp.’s Chairman Rometty’s position:

> We believe that data is the phenomenon of our time. It is the world's new natural resource. It is the new basis of competitive advantage, transforming every profession and industry. If all of this is true – even inevitable – then cybercrime, by definition, is the greatest threat to every profession, every industry, and every company in the world (Morgan 2015, p. 11).

One of the primary drivers of the change in perception of data and its value, is that information has moved from a manual process. Previously, data had a physical presence secured from outsiders, yet easily and readily accessible at our fingertips, by simply locking and unlocking the filing cabinet. The increasing use of computerised technology – particularly networked computerised technology – to generate, replicate, use, transfer, and store data has caused an increasing degree of challenge to security as it has shifted from hard copy and manual security to digital, then cloud-based, cyber security.

However, the shift from paper and manual systems to computerised and digitised systems has also shifted the locus of control of data and information from leadership and management to the technology department.

2.2.1 Technology side of cyber

Technology's importance cannot be undervalued as everyone in the organisation uses technology and everyone handles data (Hasib 2015). However, the shift of control that has occurred as a result has been identified as problematic on a number of occasions, from multiple perspectives. Yet it seems not to have been grasped as a matter of significant concern that needs to be addressed.

For instance, it has been recognised that organisations need to commit to maximising their data and its value, and therefore it deserves to be managed professionally and aggressively as a critical corporate asset (Bhatt 2000b). A core component of such management is to recognise that cyber security involves more than just IT (Goodyear, Goerdel, Portillo & Williams 2010). Yet for many years, cyber security has been seen (by organisations and by researchers) as a technological problem, for which the IT department should be responsible.

Consequently, years of cyber security 'data' and 'fixes' (and research papers) did not address the human aspect which was often viewed as the 'weakest link'. Rather they focussed on hardware, software, data communications, algorithms, and various technological responses to risk.

Warnings have been issued through past decades that there is evidence that the technology is failing its human users, not the other way around (McLeod 1992),

but it is still the case that some “technologists broadly condemn human stupidity as the root of all cybersecurity problems” (Wolff 2016, p. 11). Nevertheless, human factors (which do not necessarily equate with ‘human stupidity’) must be considered, and recent research has begun to recognise this.

2.2.2 Human side of cyber

Technology is often falsely perceived as the immediate answer to Information Security problems, (Metalidou, Marinagi, Trivellas, Eberhagen, Skourlas & Giannakopoulos 2014). However, Information Security has been identified both in practice and literature as primarily a human factors problem (Hasib 2015; Proctor, Lien, Schultz & Salvendy 2000).

Metaphorically, attackers today ignore the locked door and enter the house through an open window (Burns, Posey, Roberts & Benjamin Lowry 2017). While that ‘open window’ refers to employees, it is not due to human stupidity but to a plethora of human factors. If this is true, then it is vital to manage the human factors of information and cyber security just as carefully as the technical side – so much so that, rather than the ‘weakest link’, people need to become an organisation’s ‘strongest defence’ (Abawajy 2014).

People are not computers and if we do not manage the human side as carefully as the technical side, we will only weaken the potentially ‘strongest defence’ (called ‘the human firewall’) and cause organisational inefficiencies (Abawajy 2014; Argyris 1976; Burns et al. 2017). Unfortunately, so long as cyber security is seen as the domain of the IT department, and employee compliance as the

domain of the Human Resources department, this is problematic. IT personnel are infamous for not having been taught (or been naturally gifted in) people skills. HR personnel are primarily educated in policies, procedures, and legislation (Hilton 2016; White 2018). Neither discipline includes leadership, communication skills, nor people skills in their core skill set or discipline education. Therefore, allocating the human factors of cyber security to either of these departments is problematic.

The people of the organisation are both the users and creators of information. When leaders recognise this and take human factors seriously, then user involvement will be built into systems design from first concept. This would entail ensuring that human factors experts are involved in all stages of design to help improve usability for end users and in the long run reduce prescribed errors.

Some organisations and researchers are recognising these issues and research and education are now starting to address issues of social engineering and vulnerabilities, employee knowledge, attitude, and behaviours (KAB) regarding cyber security, and making cyber security training mandatory in a manner similar to Occupational Health and Safety (OH&S) training (Parsons, McCormac, Butavicius, Pattinson & Jerram 2013; Pattinson & Jerram 2013). While these efforts are important, they deal with only a few of all the identified issues, and they do not offer strategies to better communicate cyber security in awareness programs. Nor do they address the significance of the role of leadership in surmounting this.

2.3 Historical context: leaders and barriers of technology

In many ways, it is understandable that leaders have taken a back seat in cyber security. Historically, the trend for technology – and therefore the technologists, or IT department and personnel – to assume control over data and information access, management, and storage has shifted organisational leadership decision-making and control from leadership to IT. The roots of this originate in a mindset where IT is seen as a technical issue rather than something top managers need to be concerned about (Hasib 2015), and – as “everyone' knows – cyber security is ‘about IT’”.

Those of us in industry and various workplaces dependent upon IT saw that, without warning, the rise of ubiquitous computing shifted the ownership of data to IT and the IT department, so that its construct was now ‘technical’ rather than ‘core business’ and accessibility became severely restricted – sometimes even impossible. For example, a user requesting data now has to justify their reasoning and detail the specific data required, without any insight into the catalogue. If the user does not speak IT jargon, this caused additional barriers as the shift of data control to IT also added levels of bureaucracy and strengthened silos and siloed thinking and approaches.

The advancement of information technology cannot be reversed or downsized. Yet the technology can be outsourced, which brings its own challenges. With outsourcing, organisations often lose ownership of their strategic enterprise architecture and governance. Now, with the real threat of cyber-attack on their

doorstep, companies are bringing technology and technology management back internally with speed and urgency. But this is not a simple ‘pull-back’ mission. When organisations outsource their IT, and/or Information security, physical computing is left to deteriorate which is expensive to recreate. More significantly, the human expertise (and loyalty) is lost – and is much harder to replace.

In my experience and that of my colleagues and supervisor, in the earliest years of the 21st century, the Information Security (IS) discipline became significantly depleted as computing and IT departments took over the IS education in universities. This improvision caused a corresponding – and arguably detrimental – change of focus. The IS discipline’s core focus to its practitioners is to uplift capacities in both business and IT so they can translate between them. However, neither business education nor IT education includes this focus, and for the most part, business and IT personnel have considerable difficulty communicating with one another unless aided by an IS professional. As professionals in the industry play the role of intermediator between Business and IT (and now cyber security), this lack of IS personnel and lack of inter-disciplinary understanding are experienced as a severe drawback.

The consequent reduction in IS educated personnel has been problematic for many years but is now critical as cyberspace expands and cybercriminals thrive. These IS personnel specialised in the business-technology communication and management sphere and supported organisational leaders to obtain strategic oversight and ensure business and technology complementarity. However, the current shortage of educated and experienced IS personnel leads organisations

and their leadership bereft of the key personnel. These personnel could have bridged many of the chasms currently existing between Technology and Leadership that impede cyber security and cyber resilience. In particular, organisations now have few – if any – people able to strategically advice the C-suite about IT or cyber and leadership responsibilities in strategic cyber security.

Now, in the era of cyber threats, leadership and top management need to acknowledge that the onus for cyber security is their responsibility. Despite the shortage of specialists such as IS personnel, executive leadership needs to bridge the gap and acquire the necessary strategic, communication and business-technology complementarity required for cyber security leadership.

2.3.1 Silo mentality at organisational level

As organisations are becoming more cyber conscious and rush to make and keep their organisation cyber secure, they are hindered by a siloed organisational structure often m (Mento, Jones & Dirndorfer 2002). “Silo” or “silo mentality” has been defined as:

> a mindset present when certain departments or sectors do not wish to share information with others in the same company. This type of mentality will reduce efficiency in the overall operation, reduce morale, and may contribute to the demise of a productive company culture (Gleeson 2013, p. 11).

Since ubiquitous computing began to dominate business, IT’s non-inclusive behaviour, and technical jargon removed the business input leaving IT making key decisions – a move that threatens the organisation’s ability to align

operations with strategic direction –causing a political turf war. Critically, the siloed operating systems and structures are inevitable single points of failure for organisations (Kotter 2014).

Cyber security should not exist in its own vacuum in IT, nor should it be deployed in isolation. It must be embedded throughout the entire business for all its processes (including culture) to be realised (Colwill 2009). Only then can we break down rigid thinking and assumptions (Argyris 1998; Bhatt 2000a) to get the right people together to enable a rapid response (Ashkenas 2015) for the fast decisions critical in times of a major cyber-attack.

2.3.2 Leadership and knowledge, information and data

The value of data[1] increases as it evolves along the value chain, obtaining a strategic advantage (Zhang, Xue & Dhaliwal 2016). Consequently, organisations are now acknowledging data as a critical asset that must be managed as professionally and aggressively as other company assets (Bhatt 2000a).

Organisational information and data (the core precursors to knowledge) do not belong to one individual but to the organisation. They should be accessible in a timely fashion to all who need it and are legitimate users (Chamberlain 1991). Yet this is not what is practised, as "*ipsa scientia potestas est*" (knowledge itself is power – a phrase in attribute to Frances Bacon's Meditationes Sacrae (1597) (Debernardi 2021). Hence gatekeepers continue to erect roadblocks to prevent

[1] Data is actually the plural form of the singular datum. However, in our shifting language, data is also becoming a singular collective noun. Therefore, sometimes 'data are' and sometimes 'data is used.

access to this jewel. Yet data leaves the organisation with individuals in droves (Oppong, Yen & Merhout 2005).

Perhaps of even more significance, as Foucault proclaimed, “power is knowledge”; it is the gatekeepers with power who often decide what is and isn't knowledge. In the new cyber security domain, this is dangerous when left up to the gatekeepers who neither know nor understand how cyber security to decide what is – and isn't – relevant and align these cyber measures to business imperatives: vision, mission, strategy, and operations. Therefore, only leaders responsible for the vision, culture and organisational direction who also understand how vital interwoven cyber security is to the organisation’s wellbeing, can reasonably make ‘gatekeeper’ decisions.

2.3.3 Leadership, and the culture of trust

Trust is often understood or misunderstood as a risky up-front investment. Yet it is an essential requirement for a healthy organisation (Lencioni 2006). Less well-known, it is a critical component of successful cyber security. However, the entrenched silos previously discussed are anathema to trust, as are many current management practices.

Management and IT currently tend to distrust employees, often considered weak links and ‘insider threats that’ must be managed. Yet, inversely, many employees who are confronted by numerous security controls blocking or limiting access holds the opinion that these measures adversely impact their ability to be productive and meet their KPIs. Their worst suspicions that management and IT

want to cling to their unchallenged power are invoked (Argyris 2003). Such attitudes do not build or engender trust.

Trust – and its lack – is at the root of this problem. Trust it is business-critical and facilitates conversations about instructional reform. It also enables genuine collaboration and aid to develop a shared understanding of the reforms (Houchens & Keedy 2009).

2.4 Restating and summarising the current issues

There is a multiplicity of other issues, large and small, that must be considered when discussing the role of leadership in an organisation's cyber security. However, to recapitulate those already examined – leaders of modern organisations who wish to protect and keep their organisations safe, need to reclaim technology management leadership, particularly cyber security.

Trust has to be built and maintained between leaders and IT, leaders and employees, employees and IT, and IT and employees. Core data assets have to be made both more secure and more accessible – a truly challenging task. Employees need to be considered partners and taught to be cyber aware and cyber knowledgeable and helped to acquire strong cyber secure habits to become the organisation's strongest defence – the human firewall. Silos have to be broken down and departments and people reintegrated into systems and a systemic organisational whole that can then be resistant toward and resilient against cyber-attacks.

This is a challenge comprised of multiple huge – and for many overwhelming – goals and tasks that require leadership, change management, and cultural development. It is, as also a significant learning curve for everyone in the organisation – from the newest end-user to the highest executive. This challenge is the focus of this research. I stated above that ‘the primary thesis driving this research is that cyber security is a complex leadership issue, with multiple critical facets that must be considered systemically in relation to one another, not in isolation. The research I propose is to investigate this challenge from the point of view of leadership. The steps taken are discussed in the next section: Research Methodology and Method.

CHAPTER 3: RESEARCH METHODOLOGY AND METHOD

This chapter explains the methodology of the research and thesis. The thesis seeks to identify and address “the role of strategic leadership in the complex issue of cyber security in organisations” which summarises the research objective (rather than a “research question”) of this thesis. The primary thesis driving this research is that cyber security is a complex leadership issue, with multiple critical facets that must be considered systemically – in relation to one another, not in isolation.

3.1 Premises

This is a qualitative exploratory study. Therefore, the underlying assumptions driving and influencing research analysis must be identified and acknowledged. The core premises identified and built upon for all three phases of this research originate from Phase 1 of this study formulated by the scoping review and are as follows:

Premise #1

Strong cyber security (incorporating cyber hygiene and cyber resilience) is necessary or organisational survival and wellbeing.

Premise #1a

Cyber security is required at every level, and in every department and aspect of the organisation.

Premise #1b

Organisational cyber security must be consistent across the entire organisation. The same policies, rules, and practices must apply in and across all levels, departments, and aspects.

Premise #2

Cyber risk is an important and often unrecognised element in organisational risk management.

Premise #2a

Cyber risk is multidimensional and multi-disciplined. Cyber defence (hygiene) and resilience therefore need to be multidimensional and multi-disciplined.

Premise #3

Current cyber risk management is dangerously siloed and fragmented.

Premise #4

As an important element of strategic organisational risk management, cyber hygiene and cyber resilience are the responsibility of the organisation's Executive.

Premise #5

Currently, most organisational executives do not recognise or fulfil their role of executive ownership, accountability, and responsibility (OAR) in organisational cyber security.

Premise #6

There is a need to accelerate maturity of the cyber security domain and profession to build a strategic cyber security foundation for effective protection of organisations.

Premise #7

Cyber security has foundations in, and is dependent upon, a variety of disciplinary approaches. These include both the “hard” sciences (e.g., computing and IT) and “soft” disciplines (e.g., psychology and organisational behaviour).

Next, in Phase 2, additional principal premises addressed Executives’ failure to understand and strategically value cyber security and executive lack of trust in the CISO, which only further widens the gap in achieving cyber corporate governance ecosystem. Therefore, the following additional premises were identified and incorporated:

Premise #A1

Cyber security needs to be a business issue and fixed into corporate governance.

Premise #A2

Cyber OAR must provide an algorithm for day-to-day managerial decision-making.

Premise # A3

Cyber security as a corporate governance must be led by the highest-level executive in the organisation.

Premise # A4

Strategic cyber value must be steered by the expert in cyber security, the CISO.

Premise # A5

CEO-CISO-OAR relationship is absent in organisational cyber corporate governance.

Subsequently, in Phase 3 the question was redefined to add a new and previously unknown premise to attest that cyber security embodies protection measures, cyber hygiene and cyber resilience. This premise formulated and matured our theory that solid cyber security (resilience) requires a cyber corporate governance ecosystem.

The following assumptions were developed to explore and test the validity of this theory and the underlying premise:

Premise # B1

Cyber security needs to be embedded in corporate governance.

Premise # B2

Cyber security corporate governance must be led by the highest-level executive in the organisation.

Premise # B3

The business ecosystem and the cyber ecosystem need to be incorporated and considered holistically, at both strategic and operational levels.

Premise # B4

The Executive must elevate their CISOs to a strategic role and empowered to fulfil their responsibilities.

Premise # B5

A "cyber security corporate governance ecosystem" as a single conceptual framework has not previously been explored.

Note that these premises are represented and refined in each phase of the research and can be found Paper 1.

3.2 Research design

The overall research design for this study consisted of a three-stage predominantly qualitative approach. Firstly, a scoping review, secondly a focussed review and empirical investigation and thirdly, a synthesising, theoretical study.

Consequently, the over-arching research question is addressed in the three stages with sub-questions: Phase 1 asks the question, “what is the current understanding of leadership in cyber security across the various stakeholder disciplines and roles in today’s Australian cyber security landscape?”. Phase 2 builds on this and moves the research question to “how is the complex and multi-disciplinary discipline and practice of cyber security enacted in the experience of cyber security stakeholders in an Australian corporate (Finance-sector) setting?”. Finally, in Phase 3 the research question develops to exploring how “theory can be built upon and developed to better understand the current landscape of corporate cyber security in Australia”. To simplify this extended series of research questions, this thesis acknowledges the (umbrella) Research Objective of the full study as “exploring “the role of strategic leadership in the complex issue of cyber

security in organisations". Each of these stages will now be presented below in detail.

3.2.1 Phase 1: Scoping review

A driving motivation for the research was familiarity with the multi-disciplinary nature of cyber security and the frustrating dearth of quality literature that explores cyber security from more than one disciplinary viewpoint at a time. Therefore, I commenced with an exploratory scoping study that drew from several scholarly disciplines to better understand the complex and intricate challenge of "Leadership and governance" in cyber security. The criteria and parameters for the scoping review are presented in section 4.7.2 Sources.

The scoping review results provided a thorough list of interrelated themes and patterns of thought and behaviour in organisational cyber security. To better explore and facilitate analysis of these results, I developed a series of tentative and complex models. These models draw on and assist in clarifying the different results and visualising the gaps. They also aid in building the conceptual design of this thesis. Although not suitable for publication, many of these models are included here because they are part of the early stages of the thesis design. The foundation models that help clarify my thinking and explore the issues I was investigating are (1) current landscape cyber governance paradox (Figure 3.1) and (2) potential aspirational future state cyber corporate governance ecosystem (Figure 3.2). The resultant rich information generated new explanations and potential areas for new research (Tisdale 2016).

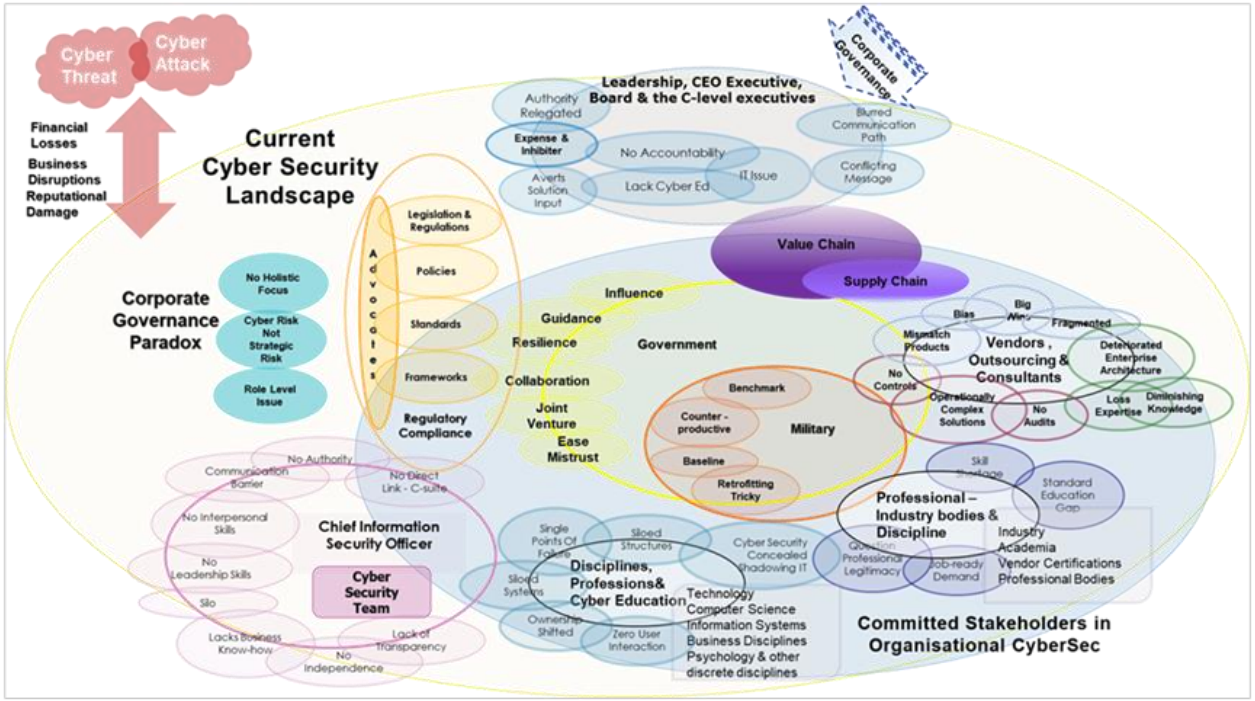

Figure 3.1.Complex model – current state corporate governance paradox

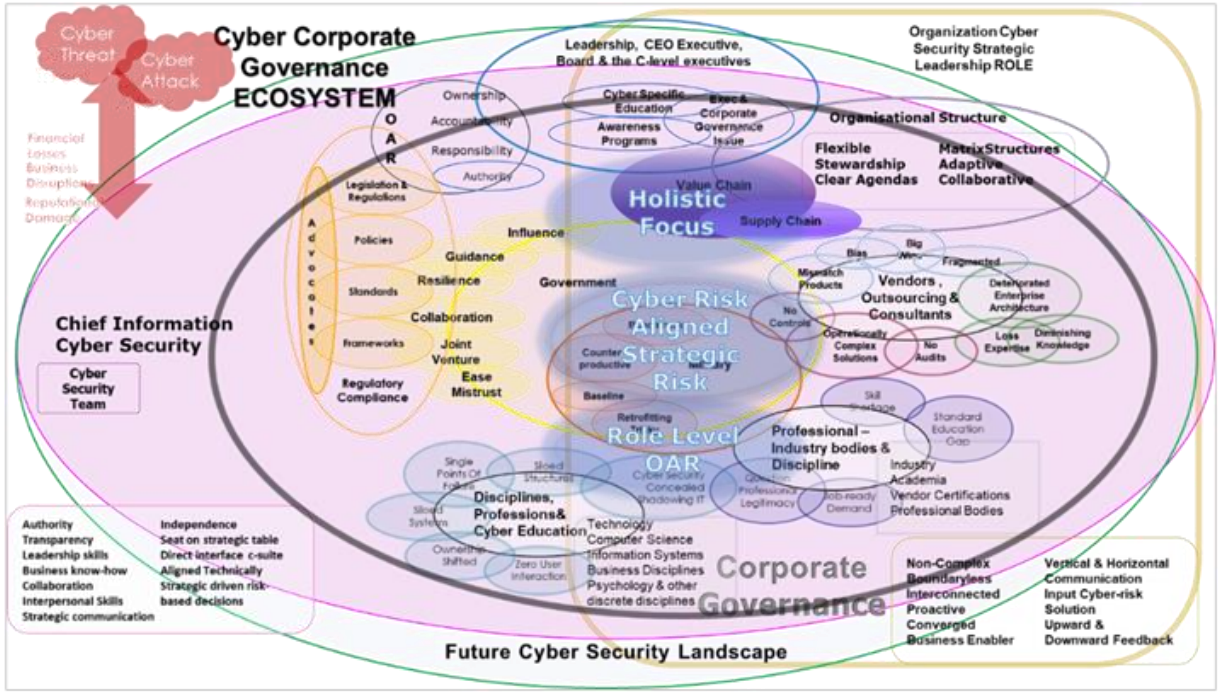

Figure 3.2.Complex model – Aspirational cyber corporate governance ecosystem

3.2.2 Phase 2: Focussed review and empirical research

The Phase 1 scoping review substantiated the need for a multi-disciplinary approach and confirmed that the aspects of cyber security leadership I wished to explore were, indeed, vital and under-researched issues. At such an early stage, an exploratory and qualitative empirical research was needed to analyse and explain a phenomenon not previously or only minimally covered by research (Ågerfalk & Karlsson 2020).

I therefore designed interview questions focused on gaining real-world perceptual insight from senior leaders, security specialists and cyber professionals through semi-structured interviews using an empirical evidence-based approach. To balance breadth and depth, I focussed on cyber security leadership in the finance sector where most of my experience had been gained.

The interview questions were built on the initial premises of the research (see Premises section) that had been verified firstly, through the scoping review and secondly in the explorative study, and finally, the illustrative models developed in Phase 1. As this phase of the research involved interviews, informed consent and ethics had to be considered and submitted to Human Research Ethics Committee (HREC). After ethics approval was granted by HREC (approval no H-2019-127), participants were invited to take part from a range of finance sector organisations including banks, superannuation, and insurance and each were forwarded details of the research objectives. Further details about the participants invited see sections 3.3.2 and 5.9 for a breakdown of demographics. See Appendix E for the list of interview questions.

3.2.3 Phase 3: Synthesis and theoretical construct

Having conducted a scoping review and empirical study to verify the research premises, the purpose of Phase 3 was to challenge the premises and findings with a strong and appropriate theoretical lens of triple loop theory. This is explained and discussed in Theoretical constructs section 6.7.1.

The combination of results from the theoretical first phase and empirical second phase allowed us to explore and synthesise our findings, in this third phase, to develop models to depict the current state of organisational cyber security and a potential aspirational future state. The process used to develop these models is explained in above in Research design section.

3.3 Research

As stated in section 3.1, a qualitative approach was the principal technique used for data collection and data analysis. To investigate strategic leadership in cyber security is an undertaking of huge scope. For scope and scale this was therefore refined to investigate the strategic leadership of the cyber security of large corporations in the Finance Sector. Large corporations have clear-cut divisions of responsibility for leaders and management, while smaller businesses are usually much more poorly resourced and at greater risk, with greater need. Although my focus is on corporations, I hope to use the insights gained to also benefit smaller organisations with less structured leadership divisions in the future. Nevertheless, the research and this thesis are specific to the corporate financial industry sector and large organisations.

The finance sector has been selected as it tends to have stringent monitoring and processes, regular audits and a recognised role of protecting client data. It is also a prime target of cyber-crime. The finance sector and sub-sectors of banking, superannuation, and insurance, provide a rational mix of organisations to allow an investigation at reasonable depth on a manageable scale.

3.3.1 Data collection

When I invited participation, I also requested access to relevant cyber security documentation in each organisation investigated including Policies, Security Operations Procedures, Guidelines, and Standards. The primary data source was interviews with those senior leaders and management responsible for each organisation's information and cyber security. Most invited participants agreed to be interviewed (with the protection of promised anonymity for the interviewee and their organisation) but did not consent to provide confidential documentation. The documentation that was promised also did not eventuate.

However, the interviews progressed well, were recorded and transcribed, and none of the participants requested that I redact any part of their interview. The Participants Interview Questions Guide is provided in Appendix E. After the interviews, I used follow-up emails and phone calls for any needed clarification during analysis.

3.3.2 Purposive sampling – participants selection

Given the focus of the research, it was evident that the CEO, CIO, and CISO (where the role exists) are critical to addressing the issue of the complexity of the

leadership role in cyber security. Of the 66 invited participants (from 34 organisation), 31 accepted (across 24 organisations). The 31 participants comprised of mixed roles and responsibilities including Directors, CEO, COO, CTO, CIO, CISO, Director IT Strategy, Planning & Governance, Head of security, IT Security Risk Managers and senior Security Advisor and consultants.

Of the study participants,16% nominated themselves as an “accountable person” for end-to-end management and cyber security decisions; 45% of participants believed they were directly responsible for developing the cyber strategy and framework while the remaining 39% of participants agreed they were actively involved throughout the cyber security process. The gender composition (6% women and 94% men) is not surprising, as cyber security remains a male-dominated field. As stated, Finance was the focus sector; a graph, demographics and details are provided in Paper 2, section 5.9, at length.

3.4 Analysis

It became apparent from the earlier stages of approaching the study that a fundamental reality of the contents of organisational cyber security was that its multi-disciplinary nature was created by the number of disparate stakeholders invested. Therefore, stakeholder theory became the foundation and primary filter for all analysis. This is discussed in section 4.13.

3.4.1 Early maps and models

The first stages of analysis were graphic; first mind maps, then models were used to illustrate and explore questions and concepts. These graphics were used

to guide the development of early ideas and findings into fuller concepts and questions. The mind maps and models from the earliest analytical stage are shared in section 2.1.

3.4.2 Thematic and pattern analysis

Building on the mind maps and models, the concepts were further developed, assisted by use of NVivo 12 Plus (released in 2018) which enabled and simplified use of thematic and pattern analysis.

Demographic data were categorised for cross-analysis with the thematic codes. Thematic coding followed ‘standard practice’ i.e., to first identify the multitude of common themes that arise – usually creating a plethora of codes –, then re-examining those themes for consistency and any clear patterns of inter-relationship. During the Phase 1 scoping review, themes and patterns were identified, coded, and mapped across the literature on cyber security leadership drawing from multiple disciplines. The criteria and details of the disciplines, journal, articles, and other resources used in the scoping review are provided Table A. 1 to Table A. 4 in Appendix A. Results and examples of the themes and patterns identified are also provided in Appendix B.

Interviews were transcribed then imported into the NVivo 12 Plus project. For rigor, each phase of coding was conducted separately. The focussed Phase 2 literature review was analysed and coded separately from the Phase 1 scoping review. The transcribed Phase 2 interviews were analysed separately from the Phase 1 coding and Phase 2 literature review codes. Three (scoping review,

focussed review, and interviewee data) had been separately coded and the results were subjected to cross-comparison, then synthesised. This procedure confirmed selected codes as all three analyses identified consistent themes and patterns. Following common qualitative practice, unusual (‘outlier’) themes were watched for to identify and catalogue, but no outliers were truly found. Instead, the consistently arising dominant themes clearly pointed to major findings both expected and unexpected.

The plethora of codes resulting from the first pass of coding, were then further analysed for commonalities, thereby significantly reducing the number of codes to a few supra-codes. These final codes represented the core findings of all three sets of thematic analysis and the synthesis of the three. These are provided in Appendix B.

3.4.3 Interpretive synthesis

Interpretive synthesis first resulted in the reduced and refined supra-codes that were the result of the final coding pass. The next stage of Interpretive synthesis introduced the theoretical lens of triple loop theory. Stakeholder theory had been the foundation and constant throughout all analysis and continued as an important element of the synthesis stage. Triple loop theory proved to be compatible with stakeholder theory as well as very relevant as a theoretical framework to guide the final synthesis. Triple loop theory and its application in this research is discussed in Phase 3 Chapter 6.

CHAPTER 4: PHASE 1

4.1 Brief Introduction to Phase 1

As stated in the introduction, this thesis is presented by publications for each of the three studies. This Chapter 4 is the first of the three papers, reporting on Phase 1 of the research.

Highlights

- Cyber security is a siloed, fragmented field.
- Disparity of agendas, approaches and lexicon augments the cyber challenge.
- Corporate governance absence is high risk.
- Executives unaware or neglect cyber-OAR (ownership, accountability, responsibility).
- Executives must acknowledge the value of cyber security and the CISO.

The reference for this manuscript is:

> Psaroulis, G., Jerram, C., (forthcoming) “The ‘Corporate Governance Paradox’ that allows silos and fragmentation to defeat organisational cyber resilience”, (submitted to Journal of Strategic Information Systems).

4.2 Paper 1. Statement of Authorship

Statement of Authorship

Title of Paper	The 'Cyber Governance Paradox' that allows silos and fragmentation to defeat organisational cyber resilience
Publication Status	☐ Published ☐ Accepted for Publication ☒ Submitted for Publication ☐ Unpublished and Unsubmitted work written in manuscript style
Publication Details	Psaroulis, G., Jerram, C., (forthcoming) The 'Corporate Governance Paradox' that allows silos and fragmentation to defeat organisational cyber resilience, (submitted to Journal of Strategic Information Systems)

Principal Author

Name of Principal Author (Candidate)	Georgia Psaroulis		
Contribution to the Paper	This paper was co-authored, but all the initial foundational work, including premises, questions, research objectives, interviews, analysis, and models, are my original work.		
Overall percentage (%)	65 %		
Certification:	This paper reports on original research I conducted during the period of my Higher Degree by Research candidature and is not subject to any obligations or contractual agreements with a third party that would constrain its inclusion in this thesis. I am the primary author of this paper.		
Signature		Date	24/01/2022

Co-Author Contributions

By signing the Statement of Authorship, each author certifies that:

i. the candidate's stated contribution to the publication is accurate (as detailed above);

ii. permission is granted for the candidate in include the publication in the thesis; and

iii. the sum of all co-author contributions is equal to 100% less the candidate's stated contribution.

Name of Co-Author	Cate Jerram, PhD		
Contribution to the Paper	Major contribution is to writing, wording, and editing. Support in development of concepts and ideas (most original ideas and concepts are Georgia's original work).		
Signature		Date	03 Feb 2022

Name of Co-Author	no further authors		
Contribution to the Paper			
Signature		Date	

Please cut and paste additional co-author panels here as required.

4.3 Abstract

This paper examines the underlying problem that leads to inefficient organisational cyber security. We explore (1) the multidisciplinary dimension of cyber risk as a new and vital element; (2) the dangers of a siloed and fragmented approach to cyber risk; (3) the role of executive ownership, accountability, and responsibility (OAR); and (4) the need to accelerate the maturity of the cyber profession to build a cyber strategic foundation for effective protection of organisations. We focus on the differences and commonalities between stakeholders and domains, the need to put aside traditional silos and coalesce as a new coherent multi-discipline to better inform organisational leaders about holistic cyber security and resilience.

Keywords: Strategic cyber security, human aspects of cyber security, cyber risk, corporate governance, fragmentation and silos, and multidisciplinary.

4.4 Introduction

This is the first of a series of three papers that explore current organisational cyber security leadership and practices. Our multidisciplinary approach and several years' investigation (spanning pre-pandemic to current 'new normal' organisations) provided insights and raised new questions. We present these using models developed to visualise and explore the current state of cyber security. This paper contributes an in-depth and comprehensive scoping review to examine the current cyber security landscape as it is presented in major academic journals. We raise awareness of issues not yet widely discussed in the literature and identify significant issues that must be researched and dealt with promptly if organisations are to develop a healthy cyber-secure and resilient future.

Cyber security in the 'new normal'

Cyber security is critical to organisational survival. The impact of the 'new normal' of COVID-19 on workplaces and a rise in remote working has made cyber resilience vital. Yet, there are limited techniques to address this gap and only a few common themes on this topic. Disastrously, the recognition and discussion of issues, and consequent approaches and suggested solutions, tend to be segregated and siloed by discipline.

A co-operative approach to cyber security, focussed on win-win outcomes, is not a novel idea (Warner 2005). However, in the second decade of the 21st century,

cyber security remains disconnected and driven by fragmented stakeholders, divided by political and strategic dilemmas, and guided by disparate policies and practices (Soundararajan, Brown, & Wicks 2019). The most prominent of these stakeholders are national and state governments allied with the military, followed closely by vendors, outsourced providers and cyber consultants, cyber education providers and professional bodies, as well as the Chief Information Security Officers (CISOs) and organisational leadership.

The imbalance of power between cyber attackers and cyber defenders is well recognised and demands a cohesive, co-operative approach by defenders to equalise the asymmetry. Organisational silos impede cyber security forming as a genuine and coherent domain (Buxton 2019), whereas the multi-stakeholder and multidisciplinary nature of these challenges needs to inspire collaboration and successful cooperative efforts (Lappi 2017) against increasingly powerful, dominant threat-actors. In this paper, we identify and discuss the disparate stakeholders and their role in the current disconnected cyber domain, particularly the paradox between the value of organisational cyber security as a strategic governance necessity and executive non-involvement.

In the theory section of this paper, we review relevant literature and outline the theoretical background describing the current cyber security landscape, the key stakeholders, and their relationships. The results section presents the principal issues and then discusses the steps necessary for a more integrated future. Finally, the paper ends with our conclusions and topics for further research.

Supplementary material demonstrating resource rigour, coding methods, and glossaries are provided in the appendices.

4.5 Material and method

Personal experience with the cyber governance paradox and colleagues' anecdotes provided us with empirical drivers to investigate this phenomenon. However, a rigorous literature search and scoping review were required to determine that the issue was a genuine research question, not one merely arising from personal bias or parochial experience. This paper describes the resultant findings and theory of that scoping review. In this section, we describe the theory, methodology, and sources used to ensure the rigour of the review.

4.6 Methodology

Our primary concerns to ensure a strong theoretical foundation for the research were those of scope, scale, appropriate theoretical frameworks, and sound balance between quality and currency of sources.

4.6.1 Theoretical construct and premises

In our qualitative research, it was important to identify the assumptions brought to the research. Premises are embedded assumptions that can indicate pre-research bias that might mislead or skew research results if not identified. Premises often form the basis of research questions and can guide rigour and depth when surfaced. The premises upon which this research is based include:

Premise #1

Strong cyber security (incorporating cyber hygiene and cyber resilience) is necessary for organisational survival and wellbeing.

Premise #1a

Cyber security is required at every level, and in every department and aspect of the organisation.

Premise #1b

Organisational cyber security must be consistent across the entire organisation. The same policies, rules, and practices must apply in and across all levels, departments, and aspects must be applied.

Premise #2

Cyber risk is an important and often unrecognised element in organisational risk management.

Premise #2a

Cyber risk is multidimensional and multi-disciplined. Cyber defence (hygiene) and resilience therefore need to be multidimensional and multi-disciplined.

Premise #3

Current cyber risk management is dangerously siloed and fragmented.

Premise #4

As an important element of strategic organisational risk management, cyber hygiene and cyber resilience are the responsibility of the organisation’s Executive.

Premise #5

Currently, most organisational executives do not recognise or fulfil their role of executive ownership, accountability, and responsibility (OAR) in organisational cyber security.

Premise #6

There is a need to accelerate maturity of the cyber domain and profession to build a strategic cyber security foundation for effective protection of organisations.

Premise #7

Cyber security has foundations in, and is dependent upon, a variety of disciplinary approaches. These include both the “hard” sciences (e.g., computing and IT) and “soft” disciplines (e.g., psychology and organisational behaviour).

4.7 Method and sources

4.7.1 Multidisciplinary scoping review

A core issue at the heart of cyber domain problems, is that cyber risk and cyber resilience are multi-dimensional and multidisciplinary. To identify and address all critical facets of the issue, research reports from multiple disciplines needed to be explored.

4.7.2 Sources

Rigour demands that high-quality literature be sourced from the various academic disciplines that inform cyber security. Given the number of relevant

disciplines, a scoping review rather than a traditional literature review was required. We identified research and gaps across the multiple disciplines that need to be considered to address strategic leadership and the role of (non-IT) leadership and management in organisational cyber security (Table 4.1). The scale and scope rapidly escalated due to the broad range of contributing disciplines. For determining rigour, the method we now describe is based on specific recommendations for scoping reviews (Joanna Briggs Institute 2020).

Cyber security is a field of rapid obsolescence resulting in the need to draw on older publications. Digital threats accumulate, morph, and advance faster than research can be conducted or published. It is therefore important to reference immediate and current “grey” literature, such as online blogs and vlogs by cyber experts. To ensure breadth, depth, and quality of references, we have referenced top-ranking journals and conferences’ publications across multiple disciplines. We used the traditional recognised rankings of business and management schools which includes articles from 47 discrete disciplines and sub-disciplines (Table 4.1). Common business school quality rankings can be found in Appendix A: Resource rigour.

Table 4.1 – Range of disciplines and sub-disciplines referenced.

# of references	Discipline or sub-discipline	# of references	Discipline or sub-discipline
5	Accounting	1	Knowledge management
3	Business	1	Leadership
1	Business ethics	1	Learning and education
6	Business research	18	Management
2	Computer-human interaction	2	Marketing and marketing management
2	Computing	1	Mathematics
2	Decision sciences	1	Operations management
2	Economics	8	Organisation studies
3	Finance (banking and insurance)	1	Production economics and management
1	Hospitality	3	Psychology
2	Human relations	2	Public administration
2	Information management	1	Public policy
8	Information systems	1	Public relations
1	Information technology	1	Sociology
1	International affairs	1	Supply chain management
1	International law	2	Systems

4.8 Analysis and synthesis

The sources named in Table 4.1 were analysed individually and together in several coding passes using qualitative coding methods. Some illustrations of dominant words and themes arising from the series of coding passes, and screenshot samples, can be found in Appendix B. Synthesis reduced the plethora of themes, and results were mapped to illustrate the major findings from our scoping review.

Roles, responsibilities, and relationships of the Executive and CISO dominated the results. We analysed, mapped, synthesised, and depicted our findings in inter-related diagrams to crystallise our results and the theoretical construct/s we present. Together, they form the theory presented in our model – *Current cyber security landscape and the committed stakeholders.*

4.9 The current cyber security landscape

4.10 Legislation and regulatory compliance

Legislation and regulations, policies, standards, frameworks, and affiliated advocates (including cyber professionals, vendors, professional bodies, and academia) drive cyber compliance and information requirements (Figure 4.1). Predefined and “limited by their own charters” (Breitrose n.d., p. 4), these operational silos impede the sector maturation that needs a cooperative stakeholder effort (Haney & Lutters 2017).

The current cyber security landscape is “a place of little regulation and considerable opportunity and danger” (Quigley, Burns, & Stallard 2015, p. 116) that exists primarily without safeguards. Digitisation has permanently altered business dynamics (Boulton 2018), rendering existing legislation unsuitable and inadequate to respond to new threats (Choo, Smith, & McCusker 2007).

The changing landscape has given rise to new “technology-enabled crime” (Choo et al. 2007, p. ix) and allows existing crimes to be committed in different ways (Thomson Reuters 2018). Legal and political redress is slower than technology advancement. The consequent delay in repercussions for cyber-crime allows criminals to metaphorically “walk through the front door” (ACS 2016, p. 17) and take over a business with little fear of prosecution (Christensen & Petersen 2017; GAP 2017).

Legal and professional regulations must set the standards needed to manage cyber risks and shape organisations’ strategy (Levit 2018). The emergence of new regulations has been slow in Australia, although the Australian Cyber Security Strategy 2020 anticipates legislative changes intended to set a minimum cyber security baseline for organisations (Australian Government 2020; Hunter 2018). Delay in legislating regulation has left organisations reliant on a patchwork of restrictive, often incoherent legal and regulatory frameworks to guide response to actual or potential security breaches and improve operational cyber security practices (Raghu 2018).

A broad regulatory lens across the overall cyber security roadmap steers organisations towards good cyber hygiene and resilience and assures

compliance to industry-relevant laws, regulations, and standards (Absolute 2019).

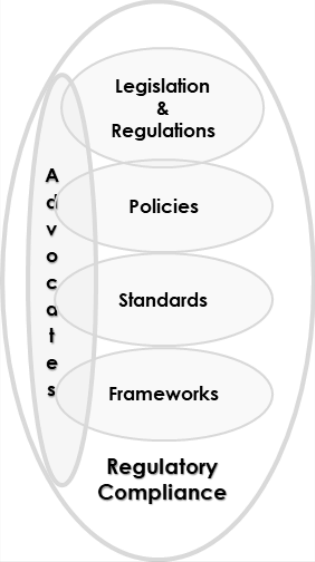

Figure 4.1. Regulatory compliance

Legislation, regulation, policy, and standards have led to frameworks that manage and solve specific problems. Advocates may specialise in one of these branches, but need to know, and relate to, others (Figure 4.1). The regulatory compliance interdependencies are critical to progress and advancement in the cyber domain (Haney & Lutters 2018). Despite efforts from a handful of advocates to uplift compliance provisions through education and training (Haney & Lutters 2018), existing benchmarks remain largely unknown.

Effective cyber security requires constant vigilance and regulatory compliance. Lack of awareness, or tentative or slow responses to cyber security legislation and regulation are risky and potentially costly (Ryan 2019). Many regard the

existing legislation as unworkable obligations (Crozier 2019), leaving anomalies and inconsistencies which delays the cyber security strategy implementation.

For the most part, governments and the military are consistent in their commitment to and investment in cyber security. Non-government organisations, however, have different structures and roles. They tend to leave security and compliance to the CISO (ACSC 2020; Ellis 2016) or the Chief Information Officer (CIO) in the absence of a CISO. In many cases, as evident in APRA's 2020 report, this leaves the CISO as the only stakeholder in that organisation's cyber security (APRA 2020).

CISOs understand the importance of regulatory compliance and are committed to staying updated with industry-relevant regulations. They know to assess the implications of new regulations and implement them into the cyber security roadmap (Stryve 2020) but are not usually in a position in the hierarchy to ensure the requisite measures are followed (Worstell 2018).

Leadership with the authority to ensure security compliance tends to be unaware of cyber security regulations or are not driven by them (ACSC 2020). When made aware, executives are often dismissive, stating "it's somebody else's problem" (McDonald 2016, p. 4) and consider their responsibility met if they "pay someone to take care of cyber security" (McDonald 2016, p. 94).

4.11 Frameworks, policies, and standards

Cyber security currently has no unified standard measure. Instead, various control objectives including frameworks, industry codes, standards, policies, best

practice, guidance, and bodies of knowledge (Wild 2018) are adopted and applied in fragmented approaches.

4.11.1 Frameworks

Frameworks play a vital role – they institute best practices for risk mitigation strategies, maintain cyber hygiene and provide insight into protecting an organisation's overall cyber health (Morgan 2020). Frameworks should be the launching point for "an open and ongoing dialogue" (NIST 2019a, p. 1) to help get all stakeholders on the "same 'measurement' page" (NIST 2019b, p. 1). There is a strong push by industry and other advocates to adopt a single and simplified security framework (Bond 2017), but duplicated and conflicting policies must first be removed.

4.11.2 Policies and standards

Security policies, procedures, standards, and guidelines help define the minimum mandatory requirements (Figure 4.1), and the baseline controls that provide guidance as to what, how and by whom (Timmermans, Roark, & Abdalla 2019) decisions are made (Pearce 2018).

Policies

"Security policy is, by definition, a set of management mandates" (Bayuk 2009, p. 3). Anchored to the organisation's core objectives (Greene 2014), policies help define the security baseline.

Policies (Figure 4.1) must drive standards and be robust enough to withstand legal and regulatory scrutiny (Greene 2014). Security policies should be determined strategically at the governance level but too often are developed in disparate siloed departments. For example, the Human Resources (HR) department writes the human compliance policy, Information Technology (IT) the computer access and privilege policies, Legal decides liability issues, Finance decides budgetary allocation and so forth across the organisation. This non-strategic approach leads to cyber security policies that lack strategic coherence, oversight, and authority and puts the organisation at risk.

Standards

Standards (Figure 4.2) set out the benchmarks and implement strong controls and regulatory compliance (Sainty Law 2017) for a consistent cyber security "approach including legal, technological, and organizational dimensions" (Elkhannoubi & Belaissaoui 2015, p. 1).

Commonly, instead of whole-of-organisation implementation, each department adopts specific cyber security clauses into the standards (if any) that they recognise are warranted by **their** department's needs.

The plethora of standards available (AustCyber 2021), have varying levels of rigour, some internationally recognised, many originating from government or military. The International Standards Organization (ISO) publications, in particular the ISO 27001, are broadly recognised as the highest level of cyber security standards available but are considered expensive and difficult to implement.

Other respected standards include the Australian Signal Directorate's (ASD) Essential 8 and the USA's National Institute of Standards and Technology (NIST).

As well as these holistic standards, there are professional and discipline-specific standards such as Control Objectives for Information and Related Technologies (COBIT) in IT and *Sarbanes-Oxley (SOX) Act 2002* for finance. Having multiple options leads to confusion and makes it difficult to decide the appropriate standards to best benchmark the individual organisation. Furthermore, there are no clear guidelines to help match specific standards to specific policies, nor are these specific policies usually aligned to an organisation's strategic goals.

4.12 The cyber security skills shortage

Government, industry, and academia concede that without sufficient expert staffing, the skills gap itself is a significant security risk. The severe shortage of cyber professionals and cyber security trained employees is a serious economic vulnerability designated a "state of emergency" (Ruiz 2020, p. 1). "The demand for cybersecurity professionals is insatiable at the moment, and this is not just an Australian problem. It's a global problem" (Franzi, in (Stilgherrian 2015, p. 2)). Although this crisis in qualified professionals was a global issue even before Franzi's 2015 statement, the deficit in cyber security professionals increases each year.

> There are an estimated 299,000 active openings for cyber security-related jobs in the United States as of August 2017. Globally, projections suggest a

> cyber security workforce shortage of 1.8 million by 2022 (Homeland Security 2020, p. 2).

More recently, Australian Cyber Security Growth Network (AustCyber) updated the 2019 Australian Cyber Security Sector Competitiveness Plan, and stated that:

> Australia may need almost 17,000 additional cyber security workers by 2026 for the sector to harness its full growth potential. The workforce shortfall has significant economic consequences. In 2017, the domestic cyber security sector is estimated to have forfeited up to $405 million in revenue, which companies could have generated if they could find enough cyber security workers to fill existing vacancies (p. 11).

The nature of the problem is broad. People in technical security roles are struggling (Chachak & Fischoff 2019) with the “clandestine nature, resource sophistication, and their deliberate ‘low and slow’ approach to efforts” (Secureworks 2017, p. 3).

In 2014, the Cybersecurity Workforce Competency Report stated:

> [There is] a competency gap between the proficiency level an individual possesses and that which an organisation desires, a professional experience gap, and an education speed-to-market gap where tertiary institutions are unable to adapt subject material in line with the speed of the changing security environment (Potter & Vickers 2015, p. 68).

Many IT personnel upgrade their technical skills in cyber security but fail to upgrade the critical “business and communication skills” (Miklai 2018, p. 41).

Conversely, business professionals who recognise the need to learn about cyber security either fear they have insufficient technical knowledge, or genuinely lack baseline technical skills.

4.12.1 Skills vacuum

The growing skills and knowledge vacuum, compounded by flawed recruitment practices, is an underlying systemic problem, centred on entry-level education and recruiting with inadequate focus on how best to hire cyber security leaders and managers. By changing the recruitment process, “non-traditional candidates” looking to break into the sector (ISC2 2020, p. 41) become available, and highly skilled, in-demand cyber professionals are retained for upcoming leadership positions.

Recruitment limitations include restrictive job descriptions demanding contradictory skillsets; too few offerings for upskilling and reskilling current employees; narrow and off-putting images and projections of cyber security careers, particularly for women; and limited and expensive education options (Robert-Edomi 2014; Ruiz 2020).

4.13 Key stakeholders in the current landscape

4.13.1 Stakeholder: Government

Governments are vital key stakeholders in the cyber security ecosystem at the local, national, and international level (Australian Government 2020; Knapp, Maurer, & Plachkinova 2017). The understaffed and under-resourced cyber

security sector continues to struggle, placing pressure on the government to lead and guide (Figure 4.2) to build greater resilience and influence the industry (Australian Government 2020; Knapp et al. 2017).

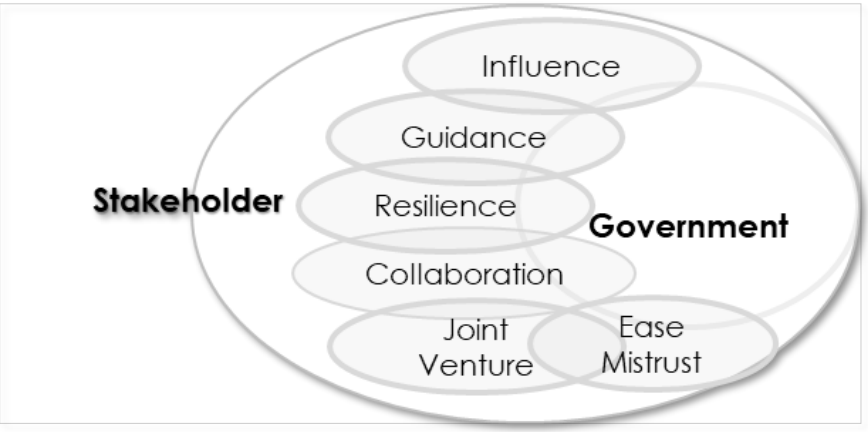

Figure 4.2. Stakeholder: Government

Governments globally take a strong lead in driving cyber security for the nation, raising cyber awareness to protect economic prosperity and national security. To influence the industry and population toward better cyber hygiene and cyber resilience, the government needs to collaborate with industry, citizens, not-for-profits, and other organisations (Figure 4.2), but due care is essential. Yielding to pressure with knee-jerk reactive policies and measures can lead to unfortunate consequences with dangerous ramifications. For instance, the Australian Government's ambiguous and controversial *Telecommunications and Other Legislation Amendment Act 2018* (TOLA Act), giving law enforcement and intelligence agencies power to access electronic communications (Adhikarl 2019), triggered national anger and fear.

The TOLA Act has implications of “Big Brother is always watching” (TAT 2019, p. 3) usurping power to surveillance organisations and violating citizen privacy. Another dangerous ramification of the hastily devised TOLA Act is the endangerment of organisational intellectual property (IP) and privacy which inhibits organisations’ ability to unlock the full economic potential, growth, and prosperity from digital disruption (Hendry 2019; Hunter 2018).

The Australian Government’s Notifiable Data Breaches (NDB) (2017) initiative received a much more positive response, as the purpose and focus is to protect privacy, not violate it (OAIC 2020). The NDB preceded international movements to protect privacy and data and aligned with Europe’s General Data Protection Regulation (GDPR) (Tankard 2016).

4.13.2 Stakeholder: Military

The military often works both with the government and academia to drive cyber security measures. As cyber security is critical to a nation’s defences in terms of cyber warfare, political safety, and national security (Australian Government 2020), the military of many countries provide standards and frameworks with strong controls. These are frequently adopted and adapted by other organisations who assume that military-grade protocols are the safest (Nova Systems 2019).

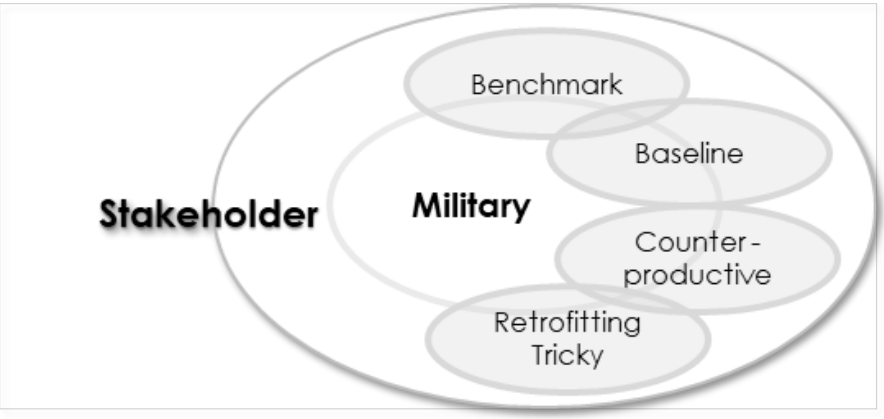

Figure 4.3. Stakeholder: Military

The military leads in the development of benchmarks, baselines, and standards (Figure 4.3) for cyber security that is rigorous and robust, based on military hierarchy, rigidity and culture which can be unsuitable for the commercial sector. As early in cyber security history as 1987, it was recognised that though the adoption of military cyber security standards and benchmarks may provide a good starting point (Clark & Wilson 1987), it requires significant retrofitting to be applicable in non-military contexts. This cultural incompatibility is still ignored more than 30 years later as organisations adopt military cyber security standards.

In Australia, the Australian Defence Force (ADF) uses the ASD's Essential Eight, considered the cyber security gold standard (Intellect IT 2020, p. 1). This standard is often used in preference to international frameworks such as ISO standards or the NIST framework.

4.13.3 Stakeholder/s (internal and third party): Value chain and supply chain

Cyber security is a borderless global issue, as are the value chain and supply chain of modern organisations. The entire value chain has become more complex, globally distributed, and intertwined into the fabric of the organisation's resources, processes, and workflows (NormShield 2019; Patnayakuni & Patnayakuni 2014). This requires, as shown in Figure 4.4, that cyber security is integrated into the value chain (Porter 1980).

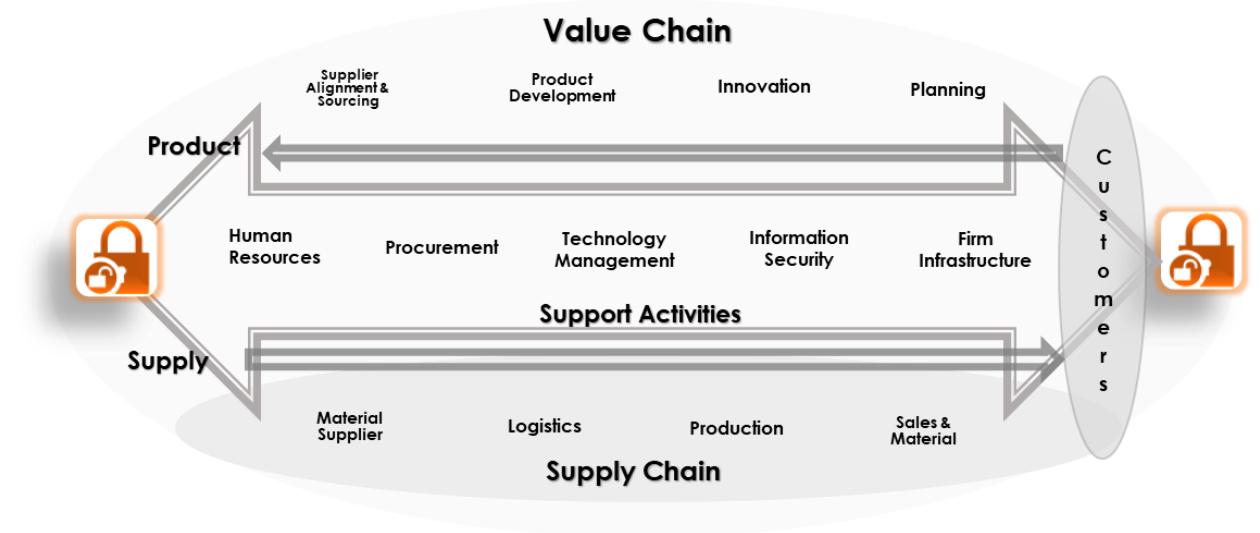

Figure 4.4. Stakeholder: Value chain and supply chain

Key value-chain stakeholders often have direct connections to an organisation's technology and access to proprietary data (Richards 2018). Mutual access to data and systems is considered a key element of the service relationship but generates vulnerabilities inherent not just at the individual entity level but as part of a global networked supply chain.

Organisations, therefore, need to ensure cyber security strategic planning encompasses the entire value chain's vulnerabilities. When organisations deal with third parties and give them electronic access to their systems, they need to recognise the inherent risk to their cyber defences (Lord 2020). Unless industry regulation and the organisation's procurement programs focus on the security of supply chain channels (Pye, Warren, Salzman, van der Meer, AustCyber, & Cynch Security 2021) (Figure 4.4) – such as instigating verifiable trust with access rights – they leave a terrible gap in the organisation's defences (Relihan 2019).

4.13.4 Stakeholder/s: Vendors, outsourced providers, and consultants.

Cyber security software vendors present themselves as cyber experts, often sponsoring and speaking at cyber security conferences and summits. "A series of thinly-disguised sales pitches" (Stilgherrian 2019, p. 3); such presentations can mistakenly mislead decision-makers who have little or no cyber security strategy expertise. By default, these vendors become the organisations' cyber experts and advisors.

This vendor-driven approach to cyber security is laden with multiple risks. Vendors' primary focus (Figure 4.5) is on constant sales and profit before investing in the client organisation's ongoing cyber security infrastructure. Such suppliers hold their own biases that influence organisations' purchasing

decisions, leading to operationally complex “systems” comprised of a mix of isolated proprietary lock-in software and solutions (Figure 4.5) (Tebbs 2019).

The move from ”vendors as providers for in-house technology” to “providers of outsourced technology service” aggravates the situation. Outsourcing – particularly the outsourcing of technology – carries specific risks. These include loss of critical expertise from the organisation (Zimmermann, Oshri, Lioliou, & Gerbasi 2018) and consequent diminishing knowledge. In turn, this leads to a deteriorated enterprise architecture (Figure 4.5) and increased cyber risk.

There are further dangers when organisations decide to rectify the costly decision to outsource by returning critical business functions and related technology controls in-house (Bjorn-Andersen & Raymond 2014). In this scenario, technology, human resourcing, and the organisation’s ecosystem are unable to recover instantly, leaving the organisation’s extended and ever-changing cyber security ecosystem vulnerable.

Figure 4.5. Stakeholder/s: Vendors, outsourced providers and consultants

Vendors and outsource providers are not answerable to their clients' regulatory sector audits or controls. Although providers do conduct quality trials (often to measure profit), client organisations rarely have access to audit results or other indicators which leaves them vulnerable and accountable for regulatory non-compliance.

4.13.5 Stakeholder/s: Disciplines, professional bodies, and cyber educators

Given the critical global shortage of skilled cyber professionals across government and all industry sectors, current and potential cyber security education providers are critical stakeholders. These include universities, colleges, technical and further education (TAFE), as well as professional and industry bodies.

4.13.6 Stakeholder/s: Disciplines and sub-disciplines

Information Technology (IT), Information Systems (IS) and Computer Science (Comp Sci) are three of the major sub-disciplines of the burgeoning field of cyber security. Most university, and TAFE science, technology, engineering, and mathematics (STEM) academic programs are developed and delivered primarily by these sub-disciplines.

Experienced researchers and teachers, usually based in Computer Science can provide strong educational foundations in the technical aspects of cyber security and its management, but usually lack knowledge, expertise, or educational offerings in the vital human and business aspects. They also tend to endorse

existing attitudes and behaviours, such as rigid siloed structures and lack of collaborative development (Figure 4.6). Such ingrained counter-productive attitudes severely hinder cyber security as a developing academic discipline and science. Subsequently, graduates transfer these attitudes to their organisations (Hoffman, Burley, & Toregas 2011).

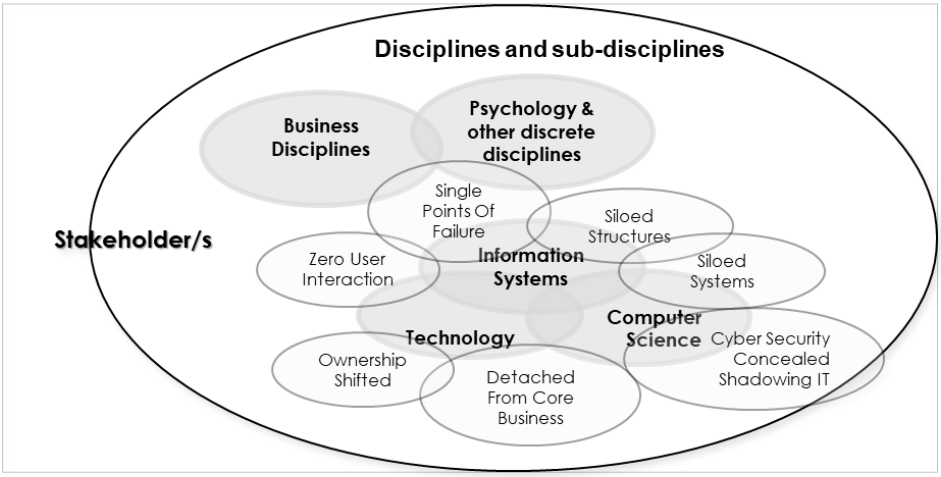

Figure 4.6. Stakeholder/s: Disciplines and sub-disciplines

The lack of acknowledgement or integration of other critical disciplines such as business or psychology (Figure 4.6) generates gatekeepers who determine priorities and boundaries from narrow disciplinary standpoints. This restricts leaders' access to correct and complete information, creating a strategic and operational vulnerability (Haney & Lutters 2018).

4.13.7 Stakeholder/s: Professional industry bodies

Professional associations and industry bodies play a crucial gatekeeper role (Suddaby, Bévort, & Strandgaard Pedersen 2019, p. 3). Well-known professional associations Information Systems Audit and Control Association (ISACA), the

Australian Information Security Association (AISA) and their strategic partner International Information System Security Certification Consortium (ISC2) collaboratively work to maintain an ongoing relationship with academia, industry, and students.

Professional associations set and maintain standards which align with and "comfortably exceed those prescribed by law" (Hoyle 2014, p. 1). Industry bodies "play an important role in representing the interest of members" (Hoyle 2014, p. 1) and improve public relations through publications and lobbying (Moyo 2016; USYD 2019). Cooperatively, these peak bodies act as negotiating or representative agencies that shape and redefine practices (

Figure 4.7).

Professional associations are entrusted to "determine the educational standards of professions" (Schrank & Young 1987, p. 1), "set clear benchmarks for acceptable professional performance" (Meintjes & Niemann-Struweg 2009, p. 11), provide governance over the legitimacy of the practice (Harvey 2004) and are primed to monitor compliance with the relevant standards (FPA 2018). Such governance is challenging in cyberspace (Reeder 2014) where security moves exponentially faster than other risk domains, and threats change by the minute.

The need for strong and stable cyber security education conflicts with the need for learning to be agile and flexible in the rapidly changing cyber security landscape, so there is a heavy dependence on highly-specific certified short

courses without the rigid credential requirements of longer programs (Reeder 2014; Townsend 2018).

To meet the growth in job-ready demand, professional bodies and educational institutions need to collaboratively ensure graduates meet the changing needs of that profession or trade (Green 2016). Professional short courses provide currency and agility. However, strong educational foundations require full university and TAFE programs taught from solid disciplinary and multidisciplinary domains.

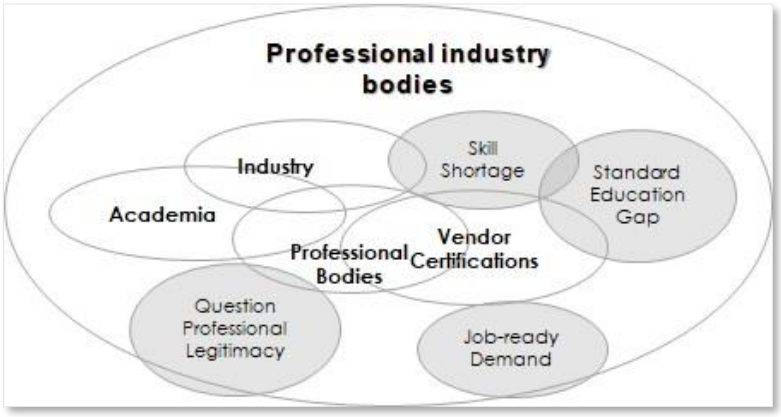

Figure 4.7. Stakeholder/s: Professional industry bodies

4.13.8 Stakeholder: Chief Information Security Officer (CISO)

Although the role is becoming more common, the CISO remains a new and ambiguous or non-existent role in organisations (Karanja & Rosso 2017; Moraetes 2017). The responsibilities, authority and budget given to CISOs differ radically (Manske 2020; Nourse 2017) depending on the organisation's level of maturity. Sometimes, the CISO's responsibilities are given to or shared by other executives such as the CIO or Chief Financial Officer (CFO).

CIO and CISO are completely different roles with competing agendas and priorities. Usually located in IT, CISOs are commonly answerable to the CIO and have no independence or authority. Unless the CIO is extremely cyber conscious, technically-driven IT priorities will override security priorities and the CISO's ability to "execute strategically" is constrained (Fruhlinger 2019, p. 3).

Designated CISOs are heavily dependent on the IT, IS and computing professions (Tucci & Roy 2019), as most CISOs come from IT and their educational background and experience usually arise from these disciplines. Consequently, most CISOs lack business and leadership training and have limited interpersonal and strategic communication skills (Figure 4.8).

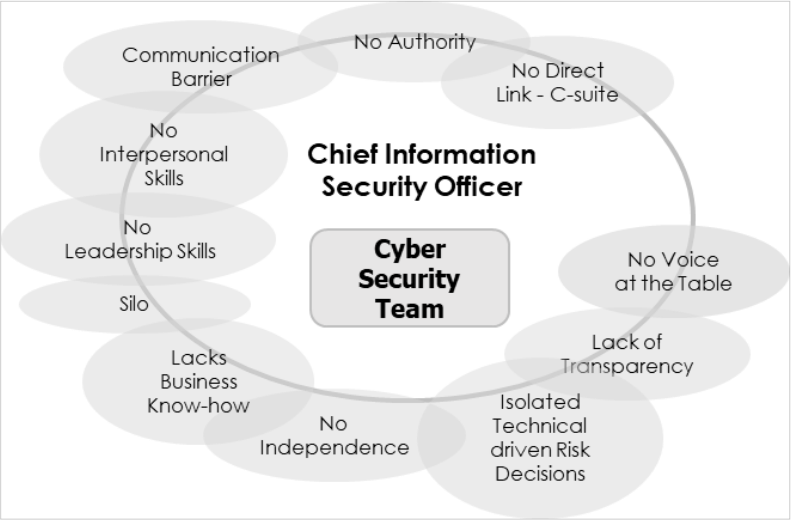

Figure 4.8. Stakeholder: Chief Information Security Officer (CISO)

4.13.9 Stakeholder/s: Organisational leadership

The most important stakeholder is the leadership group. Regulators stipulate that the CEO and Board have primary responsibility for the corporate governance of

cyber security in their organisations, but this has been slow to disseminate or implement.

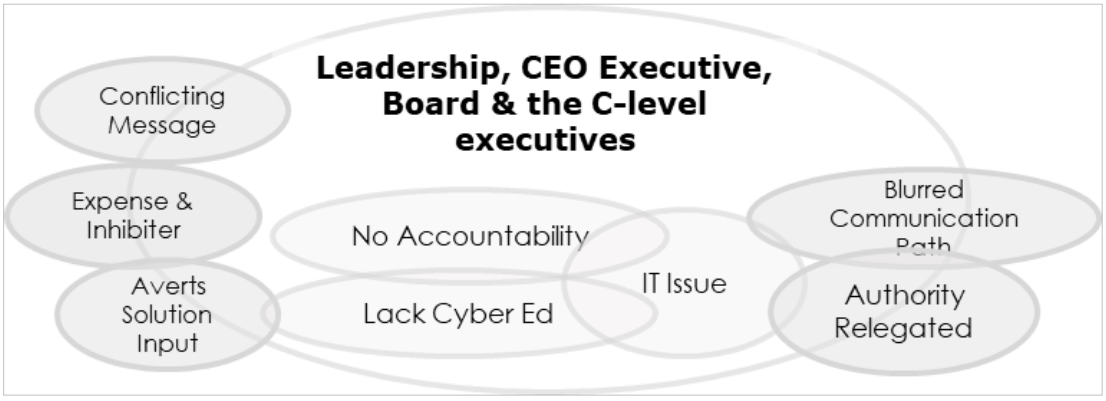

Figure 4.9. Stakeholder/s: Organisational leadership

Despite significant risks to the organisation, the Executive often places cyber security as a very low priority. “Boards either aren’t properly informed about the true state of their entity’s cyber security, or they fail to grasp why urgent action is required” (APRA 2020, p. 5) (Figure 4.9). The tone of cyber security needs to come from “the highest executive level of an organisation” (Hasib 2015, p. 5) who must mandate commitment or otherwise be guilty of “executive irresponsibility” (Benjamin 2014, p. 1).

Despite a gradual increase in awareness of cyber security in boardrooms, it “is poorly understood by the majority of decision-makers” (CGI 2019, p. 5). “Nearly half of organizations (49%) have cybersecurity on their board agenda at least quarterly” while, “only 4% of respondents say cybersecurity is on the agenda once a month, a frequency often considered a leading practice” (Deloitte 2019, p. 1).

4.14 Stakeholder analysis

Unrecognised as a burgeoning discipline, the current highly fragmented cyber security practice has siloed stakeholder clusters which continue to prevent the converged stakeholder model that cyber security demands.

4.14.1 The divergent and convergent stakeholder roles

Though closely linked to the value chain, executives often remain divorced from the other cyber security stakeholders. Where stakeholders have multiple roles in the current landscape, we portray each role separately in our models (e.g., vendors have an additional role as cyber educationalists to address the skills gap and uplift the profession).

4.14.2 Regulatory compliance as a conduit

Regulatory bodies such as APRA and ASIC have emerged as professional bodies invested in cyber security (Australian Government 2019; Deloitte 2020). This new awareness has led to significant steps in the development of cyber-specific professional responsibilities in relevant domains and is evolving as a conduit to connect cyber security stakeholders.

Legislation and regulation need “teeth” to be effective (Hasib 2015, p. 33). In cyberspace, there is a deficit of stringent national and international laws. Though organisations look to government for funding, support and guidance, cyber security legislation is sparse and largely ignored.

4.15 Stakeholder relationships

4.15.1 The government and the military

Although government and military are not the same entity, they are closely related. Government funds the military, and the military serves the government. Regardless of how they operate separately, the military and government uphold and disseminate consistently aligned cyber security policies, standards, and statements.

To build credibility, vendors and cyber consultants often draw upon and benchmark their work against ASD's Essential Eight and AustCyber resources. CISOs also tend to rely on these resources as their benchmark.

4.15.2 Vendor, professional bodies, and educators

To help address the critical shortage of cyber professionals, vendors develop relationships with educators and professional bodies. Immediate demand (Hitchcock 2007) is met with current speed-to-market training programs that can be instantly applicable in the work environment – a speed of response that tertiary institutions cannot imitate (Potter & Vickers 2015). Vendor-based certification ties the student to specific products, and the ongoing purchase-and-certification cycle creates an interdependence for clients and students to keep buying and learning.

CISOs often engage vendors as cyber advisors to tailor their organisation's needs. However, when vendors bypass the CISO and market directly to senior

executives ignorant of cyber security strategy, they can sometimes obtain CEO commitment to inappropriate products, causing added vulnerability.

4.15.3 Disciplines, professions, and educational professionals

The fundamental relationship between the disciplines, professions, and organisations that employ and manage cyber security graduates (Greef, Post, Vink, & Wenting 2017) is critical to the current state of cyber security, but problematic when these bodies have conflicting agendas and goals.

Government and military personnel have usually been educated and shaped by a particular discipline. For example, the ADF's Defence Science and Technology Group (DST) personnel work in groupings and tasks clearly based on disciplines. Most personnel in organisations have been employed for skills and roles specific to their discipline-based education or professional certification (e.g., Accounting graduates are hired to be accountants).

Almost all current cyber professionals state freely that they were not educated or employed as cyber personnel but had to step laterally from their previous roles and disciplines (usually IT, Comp-Sci, or IS) (CSOMag 2018). This invariably means cyber security personnel inherit disciplinary bias and lack other-discipline knowledge.

4.15.4 Professional associations, industry bodies and vendors

Professional associations, industry bodies and vendors are interconnected with their discipline-specific university academics in a tight, mutually constructed relationship. Although independent, these stakeholders are mutually focussed on

standards and education in their specific domain. Cyber professionals and professional bodies express mutual interest in cyber security education, and commonly perceive that only through a joint professional-academic responsibility model can the cyber skills gap be effectively addressed.

Professional associations “adapt to and try to shape” (ICAEW 2012, p. 3) and define benchmarks to meet industry expectations. They have been entrusted with determining the professional competencies (Meintjes & Niemann-Struweg 2009) and educational standards as well as providing governance that seeks to legitimise the practice (Sushanta 2017). Professional associations such as ISACA, AISA and ISC2, do work collaboratively to maintain an ongoing relationship with academia, industry, and students.

In some cases, there is acknowledged overlap between educational offerings, particularly with market-leading brands such as Microsoft, Oracle, and SAP. Professional bodies are also increasingly recognising certification by leading cyber security companies and bodies such as the SANS Institute and ISC2, to both educate and certify.

Professional associations work with and support tertiary education in a mutually beneficial relationship, often offering significant “educational discounts” on software that ensures graduates are familiar with common workplace products. Students benefit in such cases as their familiarity with the software makes them work-ready and benefits the employing organisation.

4.15.5 Chief Information Security Officer (CISO), and leadership

Of all the stakeholders, the CISO has the least access to the Executive and Board (Kiryakova 2019). The 2019 ISACA State of Cybersecurity Survey revealed only “a paltry 3 per cent” of cyber security leaders in Australia reported to a CEO (Zongo 2019, p. 3). The CISO relates to all aspects of regulatory compliance, which is key to their role, but rarely have the authority or resourcing to ensure compliance or to communicate with the Executive about compliance needs.

The CIO, who usually has authority over the CISO, may possibly – but more probably does not – have specialised cyber security knowledge or practice (Rogelberg 2016). But when the CISO has no access to strategic leadership, they are dependent on the CIO to convince executives to allocate attention and resources for strategic organisational security objectives (Enns, Huff, & Higgins 2003). Consequently, any limited funds available for cyber security tend to go directly to bottom-line hardware and software defences. On occasion, extra funding may be squeezed out to contribute to cyber hygiene, but funds are rarely made available to build cyber resilience.

4.15.6 Leadership and the value chain

Structurally, the entire value chain is vulnerable and provides avenues for successful cyber-attacks that are “inside” the firewall and other defences. Although executives understand their responsibility for the organisation’s value chain (Protiviti 2019), they do not usually comprehend the cyber risks to or

through these chains (APRA 2020). Having limited or no relationships with other cyber security stakeholders, most executives transfer all their responsibility for cyber security to the IT department, without insight or access to value-chain governance.

The resultant ignorance and denial of accountability have seen regulators introduce personal liability with civil penalties for executives who fail to perform what has now become their legal obligations (Deloitte 2020). In recent years, with the onslaught of new regulations, executives have slowly started to recognise that they, not the CISO, are accountable, but the subsequent necessary action remains slow.

4.16 Results: Principal issues

These relationships between stakeholders present a messy picture of interdependence that highlights the following principal issues:

1. Fragmentation caused by silos.
2. Inconsistent lexicons caused by siloed origins.
3. Executives' failure to understand and strategically value cyber security:
    a. Lack of corporate and strategic cyber security governance.
    b. Failure to value the strategic importance of the CISO.
    c. Inappropriate hierarchical structures.
    d. CISOs' lack of status, power, and authority.
    e. Executives' lack of ownership and accountability.
4. Inappropriate adoption of unsuitable frameworks and solutions.
5. Lack of communication and absence of feedback loops.

4.16.1 Principal issue 1: Fragmentation caused by silos

Cyber security industry fragmentation and multiple cyber disciplines combined with organisational silos and compartmentalisation of responsibilities have resulted in unclear, contentious, and confusing cyber security roles and responsibilities. Lack of communication including feedback between departments, disciplines and various other silos also cause and aggravate existing silos.

The principal issues are compilations of several sub-issues. For instance, vendors' strong influence appears to replace the role of strategic drivers of cyber

security (3a), which has arisen from the organisational vacuum caused by executives' lack of understanding and knowledge of, and commitment to, their organisation's cyber security (3b).

4.16.2 Principal issue 2: Inconsistent lexicons caused by siloed origins

The dominant themes of siloism and fragmentation in cyber security domains arise from distinct disciplines that have individual lexicons, values, goals, and approaches. Language (including jargon) is the foundation of education, and certification of education is by nature modular and discrete.

The criteria for selecting any specific certification are heavily reliant on employers' known preferences and biases. The employer might either be an HR professional without accurate knowledge of what is needed in a cyber professional, or a manager who prefers to hire employees with familiar qualifications. University and TAFE education also have an inherent silo structure offering courses in cyber security from different foundation disciplines and schools. While it is not unknown, it is extremely rare for a university to offer the multidisciplinary cross-faculty program that is truly needed for cyber professionals.

The transition from an IT background to cyber security from an operational perspective has made sense (Pompon 2017) but has created a strategic challenge. The new cyber professionals mostly lack management education or experience and have "limited knowledge of how to operate at the executive level

and speak ‘executive’ language” (Winder 2019, p. 4). It is easy to forget that “executive language” is not taught or learnt outside management circles and that there is an inherent distrust – sometimes even contempt – for professionals who do not speak that language.

Consequently, many cyber professionals who operate from a predecessors’ legacy (Tsui, Zhang, Wang, Xin, & Wu 2006) do have strategic cyber security knowledge. However, without a management lexicon, they are unable to communicate and recalibrate cyber security expectations (MRH 2015) to executives who lack a cyber lexicon. As a result, cyber practitioner roles remain non-strategic, without executive understanding or support, leading to a reactive and prevention-focussed operation (Thycotic 2019).

Principal issues 1 and 2 are inextricably intertwined. The single-discipline and old-school approaches arise because most business professionals are university educated from specific disciplines and use the lexicon of their home discipline. However, cyber security by necessity needs to be able to work across departments smoothly and cohesively with common frameworks that traverse the communication barriers to achieve a solid organisational cyber hygiene and resilience.

4.16.3 Principal issue 3: Executives’ failure to understand and strategically value cyber security.

a. **Lack of corporate and strategic cyber security governance**. Corporate cyber security governance has emerged as a dominant theme; issues of

leadership responsibility and organisational structure point to fundamental problems that have ramifications for strategic risk management and impact on culture.

b. **Failure to value strategic importance of the CISO.** Another recurring theme is the challenge of managing multiple relationships between disparate stakeholders. Executive lack of understanding leads to an organisational structure that demotes the cyber security role to a primarily IT operational level. Such a subordinate position has no strategic input and is “fraught with responsibility without oversight and accountability” (Rosenquist 2018, p. 3). This issue causes and aggravates many of the other issues such as strategic value of and budget for cyber security; role and status of CISOs; absent or ambiguous ownership and accountability for organisational safety, privacy, and wellbeing; and pervasive consequences to organisational culture.

   Cyber security is fundamental to organisational risk management and therefore a strategic responsibility, yet executives continue to have “wilful blindness” (NETJMC 2020, p. 1) about cyber security’s strategic value. If organisations are to become cyber secure and resilient, it is essential for executives – the C-suite and the Board – to understand the vital nature of organisational cyber security as Risk Management.

c. **Inappropriate hierarchical structures**. In a rigid organisational structure, bureaucracy proliferates, and organisational charts expand and have competing agendas (Zook 2016). These create additional silos that slow down communication and hinder critical upwards feedback, thus increasing executives' inability to comprehend, and align strategic and operational cyber security issues (Stackpole 2017; Zardini, Rossignoli, & Ricciardi 2016).

d. **CISO's lack of status, power, and authority**. The most significant organisational issue that impacts cyber security is the role of the CISO in rigid hierarchical structures.

   The current reporting relationship, in which a CISO usually reports to a CIO, is strategically unsound and problematic due to distance from strategic decision-makers. The two roles are misaligned with competing priorities, budget constraints and tensions between ICT operational needs and cyber security demands.

   The potentially conflicting political structure of CIO versus CISO blocks productive communication and creates competition. This common conflict is heavily intertwined with other principal issues discussed in 3a) and 3b). As long as the CISO is a subordinate operational role, and executives have no comprehension of either cyber hygiene or resilience, the CISO

will remain unable to provide the organisation-wide cyber security expected.

e. **Executives' lack of ownership and accountability**. Organisational consequences of executive failure to understand and strategically value cyber security include attitudinal and behavioural lack of ownership and responsibility for cyber security. The consequent approach to relegate all cyber security responsibility to the CIO or CISO, only reinforces an ad hoc approach that fails to recognise cyber security as a business issue (Maynard, Onibere, & Ahmad 2018) thereby permitting the Executive to avoid responsibility (Westby & Allen 2007).

4.16.4 Principal issue 4: Inappropriate adoption of unsuitable frameworks and solutions.

Ironically, all the sub-issues comprising Issue 3 often lead to the adoption of unsuitable frameworks and solutions. Under-budgeted CISOs purchase and create multiple ad hoc solutions and partial solutions which they then have to piece together.

Another challenge in selecting an appropriate and workable framework is the lack of an official standard and little guidance for understanding which, of the plethora of popular frameworks, are appropriate in which context. Executives' lack of knowledge and CISOs' lack of strategic language, escalate the confusion.

4.16.5 Principal issue 5: Lack of communication and the absence of feedback loops.

Finally, there is a recurring lack of communication between strategic decision-makers, managers, and operation-level cyber security personnel.

The absence of feedback loops due to lack of communication results in the inability to analyse decisions and consequently an increase in vulnerabilities, risks, and threats. In any risk management domain – not just information risk – an inability to receive and use feedback at all levels (strategic, management, and operational) is catastrophically dangerous.

4.17 The current landscape: Synthesis view

Following four passes of coding, we mapped the models (Figure 4.1 to Figure 4.9) to clarify principal cyber security stakeholders and their interrelationships. This synthesis allowed us to understand current organisational cyber security as a landscape of fragmented interactions impeded by overlapping but dissociated silos (Figure 4.10), which we originally designated the *Current cyber security landscape and the committed stakeholders* but renamed – after analysis – *Cyber governance paradox*.

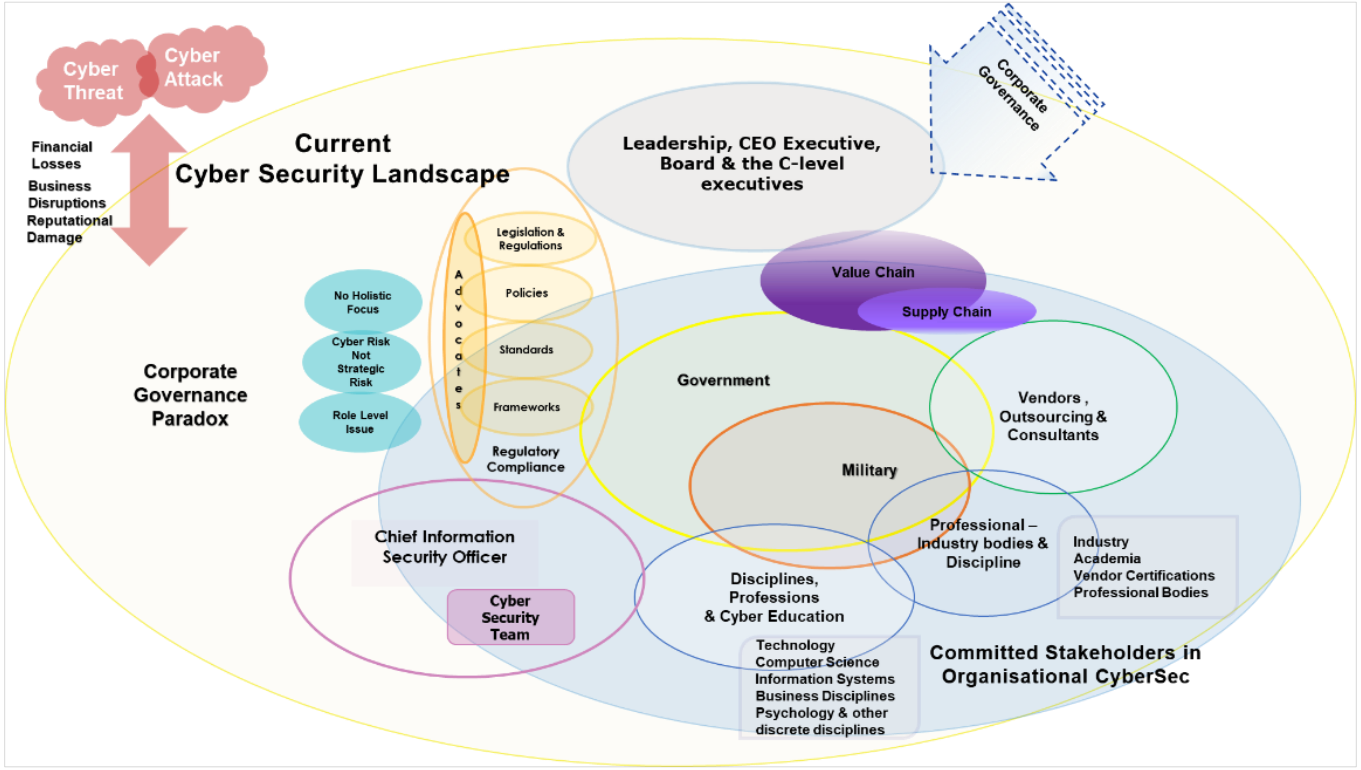

Figure 4.10. Simple model – current cyber security landscape and the committed stakeholders

The synthesis and model (Figure 4.10) reinforced the findings that the absence of corporate governance is a significant and driving factor behind many of the issues. This core aspect, “Cyber governance paradox” (Figure 4.10), is represented by the underlying pale yellow elliptical shape. Previous models did not show this aspect, as its identification arose from the synthesis of the component models.

Leaders (Figure 4.10) have set themselves apart from cyber security stakeholders other than the value chain – a recognised area of corporate governance in management circles, thus the “paradox” in the title. Embedded in the ‘Cyber governance paradox’ (Figure 4.10 top left), but outside of the ‘committed stakeholders’ (pale blue elliptical) are three important findings (blue ovals). These findings: (1) lack of holistic focus, (2) cyber risk not considered strategically, and (3) the dangerously inappropriate roles and status of cyber security, CISOs and executives, testify the absence of corporate governance. This combination generates strategic and operational gaps that engender the need for a unified cyber corporate governance ecosystem.

Theoretically, leadership is responsible for their organisation’s corporate governance. However, as Figure 4.10 illustrates, cyber security governance remains outside the circle of influence of the other primary stakeholders. Given the choice and adequate resources, most CISOs would be fully engaged as “committed stakeholders”. Yet, like the Executive and due to Executive decision-making, the CISO (pink, mid-left) is also somewhat apart. Due to a lack of

resources, CISOs primarily participate as a peripheral “committed stakeholder” which they manage through attention to regulatory compliance and involvement with IT.

Government and military are centrally placed (Figure 4.10) as recognised leaders in cyber security. Most other stakeholders are also fully within the sphere of “committed stakeholders”, overlapping with government and military and each other in a pattern of shared disciplinary and professional interest.

For a full depiction of the diagrammed theoretical construct with details, see in Appendix C.

4.18 Discussion: towards a more integrated future

The current landscape of cyber security is not a healthy one. Successful cyber-attacks on organisations without strategic cyber resilience are catastrophic both financially and to brand image. Yet, the ‘cyber governance paradox’ model (Figure 4.10) clearly illustrates that current practice and interrelationships are not adequate for the multidisciplinary needs of organisational cyber security.

The key issues identified in this paper have more than theoretical significance and must be addressed with some urgency for organisational cyber (and economic) resilience. Unless the CISO is recognised as a trusted strategic partner in corporate governance, the ever-increasing number and strength of cyber-attacks will inevitably put the resultantly vulnerable organisations at huge ongoing risk. For an organisation to be genuinely cyber resilient, adequate status, budget, and strategic input by the CISO is paramount.

The ability of the CISO to protect their organisation is determined by the Executive. To be cyber secure, executives must step up to their required OAR (ownership, accountability, and responsibility) in relation to their organisation's cyber security. However, when the CEO and Board abrogate their OAR, they create a vulnerable, immature culture in terms of modern cyber reality.

The ramifications of retaining a fragmented legacy of a siloed approach to cyber security are significant. Fragmented cyber defences are akin to a defensive wall comprised of bricks and wire to defend against modern rocketry. The result is severe risk to client and employee privacy, loss of finances and intellectual property and other corporate secrets.

Cyber security stakeholders urgently need to take a united, holistic approach. Until a united multidisciplinary approach to cyber security becomes the norm, mixed and competing lexicons will continue to confuse communications and disrupt effectiveness. Furthermore, egos, ignorance and old-guard gatekeepers will prevent adequately multi-pronged and cohesive cyber security for organisations.

We contend that universities, disciplines, and the professions – supported and encouraged by government – must jointly take action to break down the barriers and deliberately build a new multi-discipline (and profession) of cyber security.

In doing so, cyber resilience would become widely available – even the norm – for all entities including government, private organisations and individuals needing cyber resilience.

4.19 Limitations and future research

We recognise that these are challenging recommendations and that they are based on research that has multiple limitations, primarily.

Scoping review. A scoping review is limited as the level of depth must be sacrificed to leave room for the needed breadth of this multidisciplinary field.

Discipline infancy. The multidisciplinary cyber security domain is still in its infancy, dependent on grey literature for currency. Only rapidly published rigorous research can alleviate this limitation.

No empirical evidence. As only phase 1 of a large study, empirical support is still to come, a necessary progression, but still a limitation.

Early-stage models. Models presented in this paper are findings from only the first stage of the research but illustrate major findings upon which the next stage of research will be built. Significant refinement is required and is a current limitation.

These limitations will be addressed in Phases 2 and 3 of this study. They also offer potential areas of exploration for other researchers.

4.20 Conclusion

This paper presents the results of a rigorous scoping review and theoretical models which depict the current landscape of organisational cyber security proffering a multidisciplinary view of important issues that need to be addressed.

These issues all need further research. Principally, there is an urgent need to commit to a coherent, multidisciplinary strategic approach to cyber security.

To enable a strong and holistic multi-discipline of cyber security, all contributing disciplines, professions and other stakeholders must put aside traditional silos. Universities and workplaces must agree on a common lexicon that enables intelligent and intelligible communication between the different branches of cyber security and between business and cyber personnel. In particular, the lexicons and approaches of strategic planning and cyber security need to be aligned in discussion, in practice, and in the Board room.

The role, status, and budget of the CISO must be immediately addressed, with organisational executives acknowledging the importance of cyber security. Finally, executives must take their governance role seriously by taking ownership, accountability, and responsibility for their organisation’s cyber security.

CHAPTER 5: PHASE 2

5.1 Brief Introduction to Phase 2

This Chapter 5 is the second of the three papers, reporting on Phase 2, an Empirical study built upon the findings and tentative models from Phase 1 of the research.

Highlights

- Organisational cyber security is a complex problem.
- CEO-CISO-OAR relationships are problematic and impede cyber governance & resilience.
- Governance mechanisms aggravate the CEO-CISO-OAR relationships.
- CEO & CISO must work in unity on OAR relationships & governance mechanisms.
- Cyber governance ecosystem' recommended as pathway to cyber security and resilience.

The reference for this manuscript is:

> Psaroulis, G., Jerram, C., (forthcoming) "Which comes first? The CEO and CISO roles and responsibility? Or the principles of OAR? (ownership, accountability, and responsibility)" (submitted to Journal of Strategic Information Systems).

5.2 Paper 2: Statement of Authorship

Statement of Authorship

Title of Paper	Which comes first? The CEO and CISO roles and responsibility? Or the principles of OAR?
Publication Status	☐ Published ☐ Accepted for Publication ☒ Submitted for Publication ☐ Unpublished and Unsubmitted work written in manuscript style
Publication Details	Psaroulis, G., Jerram, C., (forthcoming) Which comes first? The CEO and CISO roles and responsibility? Or the principles of OAR? (submitted to Journal of Strategic Information Systems)

Principal Author

Name of Principal Author (Candidate)	Georgia Psaroulis		
Contribution to the Paper	This paper was co-authored, but all the initial foundational work, including premises, questions, research objectives, interviews, analysis, and models, are my original work.		
Overall percentage (%)	65 %		
Certification:	This paper reports on original research I conducted during the period of my Higher Degree by Research candidature and is not subject to any obligations or contractual agreements with a third party that would constrain its inclusion in this thesis. I am the primary author of this paper.		
Signature		Date	24/01/2022

Co-Author Contributions

By signing the Statement of Authorship, each author certifies that:

i. the candidate's stated contribution to the publication is accurate (as detailed above);
ii. permission is granted for the candidate in include the publication in the thesis; and
iii. the sum of all co-author contributions is equal to 100% less the candidate's stated contribution.

Name of Co-Author	Cate Jerram, PhD		
Contribution to the Paper	Major contribution is to writing, wording, and editing. Support in development of concepts and ideas (most original ideas and concepts are Georgia's original work).		
Signature		Date	03 Feb 2022

Name of Co-Author	no further authors		
Contribution to the Paper			
Signature		Date	

Please cut and paste additional co-author panels here as required.

5.3 Abstract

We report the second phase of research into organisational cyber security leadership, and explore critical issues identified in Phase 1, including the role and relationships of the Chief Executive Officer (CEO) and the Chief Information Security Officer (CISO) and the complex problem of Ownership, Accountability, and Responsibility (OAR) of organisational cyber security. Based on a focused literature review and qualitative empirical semi-structured interviews, our data revealed socio-political obstacles that aggravate the OAR and the CISO and CEO issues. We found that corporate governance and its mechanisms must be simultaneously addressed and better aligned to the CEO-CISO-OAR relationships to achieve organisational cyber security and resilience.

Keywords: Cyber security, corporate governance, Executive (CEO and Board); Chief Information Security Officer (CISO), principles of OAR (Ownership, Accountability, Responsibility), Governance Mechanism.

5.4 Introduction

Cyber security is being acknowledged as a strategic and operational problem by several forward-thinking executives, including cyber thought leaders and experts. Chief Information Security Officers (CISOs) are gradually evolving to executive positions and becoming more visible and influential. In a similar trend, we find glimpses of high profile cyber aware Chief Executive Officers (CEOs) and CISOs advocating cyber security strategic direction. Yet these cyber leadership trends are not the norm in practice.

This paper, Phase 2 of a multi-year study, reports on an empirical investigation into the level of Executive and strategic corporate governance in organisational cyber security. Our focus is on Executive commitment to cyber security, and the relationship between the Executive (the CEO and Board) and the CISO. We build on our previous research published in (name withheld for review (nwfr)) and present our argument that the “aspirational future state of organisational cyber security will be embedded in cyber corporate governance”. Our prior research revealed major factors affecting cyber security and impeding development of healthy cyber resilience are (1) Executive perception of cyber security and therefore of the CISO; and (2) absence of corporate governance of cyber security (the ‘cyber governance paradox’).

An evidence-based approach is taken to investigate Executives’ understanding and strategic valuation of cyber security and their trust in their CISO as a

strategic partner. The study explicitly explores where the cyber security OAR (ownership, accountability, and responsibility) resides. It investigates the relative obligations of the CISO and the Executive, and the role of OAR in the cyber governance domain. Finally, the study clarifies the impact of cyber security corporate governance on the relationship and roles of the Executive and the CISO.

We first present relevant literature on current cyber security practice, key stakeholders, their relationships, and the complex issues of cyber-OAR. Next, the Results section provides an overview of the empirical research into organisational cyber leadership, followed by a discussion of our findings, conclusions, and recommendations that lead to future research.

5.4.1 Cyber security: technical or business issue?

Whether cyber security is a technical or emerging business issue is an ongoing debate. Many CEOs still do not understand the strategic value of cyber security or necessity of cyber resilience. Claims that cyber security has become a strategic issue are therefore questionable. In many organisations, CISOs still lack the requisite strategic recognition, status, authority, and power to build cyber resilience into the organisation’s governance and practice or partner the Executive to do so.

A shift in perception from “technological to managerial tactics to a strategic approach” to cyber security (Althonayan & Andronache 2019, p. 1) has accelerated the need for a strategic Board-level response to the current cyber-

risk environment. However, little is known about the Executives' role in overseeing risk management, particularly cyber security and other IT risks.

Over a decade ago, it was claimed that the failure of the Executive and Boards to understand the depth and breadth of cyber security had led to a misunderstanding of the security problem. "For most boards, cybersecurity is far from a core competency" (Chertoff 2018, p. 1). This results in "the wrong problem is addressed" (Bakari, Tarimo, Yngström, Magnusson & Kowalski 2007, p. 53). The notion "little is known" is a serious understatement of the Executive's competency (Lankton, Price & Karim 2021), indicating a need to deploy a strategic Board level response to cyber-attack.

Our research seeks to substantiate our claim that 'the wrong problem is being addressed' and this cyber issue remains true today for many organisations. This misperception and the incorrect responses adds to the conflict and strategic misalignment of the key stakeholder roles of the CEO and CISO. This insight is pivotal to our research.

5.4.2 Stakeholder theory

To understand the complex issues of OAR, and the Executive and CISO relationship, we have drawn on stakeholder theory. Stakeholder theory is concerned with understanding who has input in the value-based decision-making process (including trade-offs) and knowing how to engage the inner circle to gain support, buy-in and commitment to create and capture value (Freeman, Phillips & Sisodia 2018).

At first glance, the two principal stakeholders of CISO and the CEO seem to have identical agendas of protecting their organisation and enabling it to survive and thrive. In reality, these roles have been in conflict and misaligned strategically.

In our first paper of this series (nwfr), we discussed multiple stakeholders in organisational cyber security. This paper focuses on the two key stakeholders, the CISO and the CEO. Designated by their title, the CISO is a key stakeholder responsible for the organisation's information (cyber) security. The CEO is a key stakeholder as the individual responsible for corporate governance and the organisation's wellbeing.

5.4.3 Cyber security and leadership

Leadership is widely recognised as a challenging and complex role. If we add the intricacy of cyber security into the mix of the well-known leadership challenge, complexity and challenges are increased. If we then add Bakari's claim that "the wrong problem is addressed" and Chertoff's statement that "[f]or most boards, cybersecurity is far from a core competency" (2018, p. 1), it is easy to understand why the role and responsibilities of cyber leadership remain ambiguous and open to interpretation (Mardis 2015).

Corporate governance entails, among other things, ownership, accountability, and responsibility, which we refer to here as OAR. It is commonly accepted that the Board and the CEO are responsible and accountable for the wellbeing of their organisations (Von Solms & Von Solms 2018).

Cyber security and cyber resilience are integral to corporate well-being, therefore to corporate governance and therefore the CEO's responsibility (Von Solms & Von Solms 2018). Moreover, it is a legal responsibility as delineated in parliamentary Act and regulatory standards such as CPS 234.

To establish clear accountability and provide appropriate governance structure with the aspirational goal of cyber corporate governance, the roles, and responsibilities of the CEO and CISO in cyber security need to be defined (Williams 2007)

The CEO

CEOs are the decision-makers in their organisation and wield dominant power over employees. They also hold a prominent position on the Board and influence the strategic building on – or rejection of – antecedents in their business model (plan and action) (Zacharias, Six, Schiereck & Stock 2015). Furthermore, the CEO characteristics of tenure, formal education, prior career experience, and positive self-concept significantly shape the firm's strategic actions (scope, risk, and change) and impact the future performance of the firm (Wang, Holmes, Oh & Zhu 2016).

The CEO's strength as the organisational leader has been built on areas of personal knowledge and expertise (Chen, Kang & Butler 2019), such as financial management. Rarely does a CEO rise to leadership from IT or other technology domains (Press 2015), so CEOs commonly fail to recognise IT as a strategic or leadership responsibility. Rather, they usually delegate IT issues and decisions to

operational managers. Consequently, CEOs and strategic leaders see cyber issues as not their responsibility. Until recently, even CIOs and other technology experts considered cyber security primarily a technology issue and not the CEO's concern. CEOs and other executives have therefore been slow to recognise that cyber security – and cyber resilience – are very much strategic Executive domain issues.

This tardiness in recognising cyber resilience as a corporate governance issue is solidly grounded in common sense inappropriately applied. To understand why intelligent, educated leaders can be so slow to recognise that cyber resilience is a strategic matter and part of their corporate governance responsibility, we draw on neurological/education science, psychology and system thinking theories. These include primary and recognised ignorance (Roy & Zeckhauser 2015), the Dunning-Kruger Effect (Dunning 2011), decisions-under-uncertainty (Farnam Street 2013) and mental shortcuts (Tversky & Kahneman 1974).

The high diversity in managerial experience across the boardroom permits multiple perspectives and represents an essential source of non-overlapping knowledge in the face of complexities (Chen et al. 2019). Until recently, however, that diversity of non-overlapping knowledge rarely included IT or cyber security. Recent claims point out that the lack of cyber fluency constitutes grounds for the (Executive and Board) to "gain the needed expertise for overseeing cybersecurity by increasing engagement with the chief information officer (CIO) and chief information security officer (CISO)" (Lankton et al. 2021, p. 116). We agree with this claim but suggest that it is not enough.

Decision-making uses existing domain knowledge to interpret what is observed (Pettigrew 2012). However, this does not necessarily transfer to the cyber security domain when the decision-makers have no ‘existing domain knowledge’. Expert decision-makers who “follow templates and decision-making shortcuts [in] their current ‘knowledge corridor’” (Wang et al. 2016, p. 823) are actually hindered by expertise and experience inappropriately applied to an unfamiliar domain. This makes it “harder for them to learn and perform in other domains” (Wang et al. 2016, p. 823). The strongly established mental patterns that are such a strength for decision-makers operating in their own sphere can be detrimental to their ability to cede expertise-based decision-making (Dunning 2011; Tversky & Kahneman 1974).

These theories regarding expert decision making and mental shortcuts explain why capable, experienced CEOs fail to demonstrate their usual strategic decision-making strengths when dealing with cyber issues. For instance, a systematic approach that implements measures to cope with a wide range of risks, such as threat modelling, is rarely applied in the face of multi-criteria complex cyber security decisions (Shreeve, Hallett, Edwards, Ramokapane, Atkins & Rashid 2020).

For a long time, despite severe fiscal and reputational damage, dramatic breaches that harmed organisations did not particularly concern CEOs or Boards. They dismissed the events as ‘not their fault’. Rather than be accountable as leaders, they adopted the victim role, along with their organisation.

However, it is only in the last few years through legislative enforcement such as CPS 234 that government and regulatory bodies have made it clear the Executive (CEO and Boards) are ultimately responsible for their organisation's cyber security. These measures hold them personally "liable for 'egregious' cyber-security negligence" (Visentin 2021, p. 1). These regulations have forced executives to recognise that the onus for their organisation's cyber governance (Neely, Lovelace, Cowen & Hiller 2020) is on them.

Yet regulatory measures do not address the other foundations for executive discomfort with cyber-OAR. A recurring theme across multiple studies in recent years is that cyber security remains outside the general governance mandate because competent and experienced executives simply don't understand it (Von Solms & Von Solms 2018) enough to make sound cyber risk decisions.

Just as CEOs understand critical success factors of effective corporate governance (Tan, Ruighaver & Ahmad 2010), they also understand the fundamental interrelationships of strategic, tactical, operational, and contingency plans and practices that enable sound decisions in their domain. This combination of knowledge and expertise is what has brought them to senior leadership.

Given cyber security is core to the day-to-day business operations and a subset of Corporate Governance (Tan et al. 2010), the Executive must now acquire the same competencies in cyber security. However, this cannot be done in isolation; it needs to be integrated into the organisational design and sit as a permanent

item on the Board agenda, interwoven inextricably with all other aspects of corporate governance (Lankton et al. 2021).

The CISO

The other key stakeholder in organisational cyber security, the CISO, is the subject-matter expert focused on information systems and technology security and compliance. In recent years, however, many have broadened their niche to also become experts in the human and behavioural aspects of cyber security.

Thus, the CISO is placed in the unfortunate position of being the ‘sole’ scapegoat if there is a cyber-disaster (Daud, Rasiah, George, Asirvatham & Thangiah 2018). This predicament is clearly in direct opposition to the thesis of our paper that the OAR of organisational cyber security must ultimately reside with the Executive. We therefore need to carefully consider the role of the CISO in organisational cyber security.

The CISO function has traditionally been the responsibility of corporate IT. In recent years, the responsibility has shifted to the role of CISO (Karanja & Rosso 2017), usually residing within the IT department and reporting directly to the CIO, and generally perceived as a specialised subset of IT with a technological security focus. This glorified techie function holds no authority or input into corporate governance, so precludes the CISO role from being considered strategic.

The CISO’s incorrect positioning is problematic. The paradoxical position of the CISO being employed in an operational role yet held responsible for the strategic

governance of the cyber function (Daud et al. 2018), has impeded organisational cyber security development.

Despite the ‘Chief’ in their title (Davidoff 2019), CISOs lack the autonomy and authority (necessary prerequisites for shaping strategic approaches to operational responsibilities) that come with this (non-) executive-level role. The identity crisis of the CISO as an “operational-techie” is further compounded by the failure to recognise the important role the CISO needs to play in business strategy formulation (Karanja & Rosso 2017).

Even after COVID-19 brought the CISO role to the fore, the CISO still lacks the strategic recognition, authority and power needed to bring cyber security concerns to the boardroom (Kappers & Harrell 2020) and the role is still not valued at the executive level (Fitzgerald 2018). Steps to redefine the role and job description with the right level of responsibilities need to be taken (Karanja 2017) to elevate the CISO to a strategic position as a respected member of the C-suite (Kappers & Harrell 2020).

5.5 Method and approach

Our study design was based on in-depth semi-structured interviews formulated through a scoping review followed by rigorous literature search. This decision was based on our previous research (nwfr) that identified the CEO (Executive level) and the CISO positions as the two leading roles in organisational cyber security governance. CEOs and CISOs could therefore provide real-world insight as cyber leaders.

5.5.1 Participants and research questions

We sought insight from cyber advocates, thought leaders, and experts. The questions we developed explored the complex cyber leadership issue and gain insight into how the cyber security leadership role is defined, determined, and enacted in organisations (see Appendix E).

This research was conducted as approved in **HREC # H-2019-127**. We recruited 31 respondents, primarily through a recruitment email detailing the research objectives sent either directly or via LinkedIn. We emailed applicants to confirm the date and time for a 60-minute interview via Zoom. Of the 31 participants, 29 gave permission to be recorded, and two consented for notes to be taken.

5.5.2 Data analysis and coding

Recordings were transcribed verbatim following the interview. Each participant was assigned a unique pseudonym. In the first pass of coding the dataset, duplication and ambiguity were removed, and demographics were categorised to enable cross-analysis. Next, a series of qualitative analysis passes were completed: firstly, identifying patterns and defining common themes; secondly, refining these codes, determining keywords and dominant recurring themes including subthemes and ‘outlier’ themes.

We sorted the responses into categories, dominant themes, and sub-themes by frequency, relationship, and underlying meaning of common word concepts and themes used by participants (see Appendix G for examples). Codes and themes

were then refined to a few supra-codes identified by a synthesis of iterative patterns, core categories and unique themes.

5.6 Literature review

Central to this research is the short-sighted view that cyber security is a technical rather than a business problem. Following an extensive scoping review (nwfr), we identified the Executive and the CISO positions as the two leading roles. Our literature review explored the key focus questions of this paper: ‘Who has authority?’ ‘Who is accountable?’ and ‘Where does responsibility reside for organisational cyber security governance?’

5.6.1 Core search

Our initial scoping review revealed a frustrating lack of quality academic publications that addressed the cyber governance issues at the heart of this study. Our subsequent rigorous updating of that review, and the more focused literature search for this paper, revealed the same dearth of relevant quality literature. Our need to draw on older publications and grey literature is a strong indicator of the need for this research.

5.6.2 Focused search

We completed a detailed search across multiple databases (Appendix H) explicitly referencing credible, reliable, and peer-reviewed literature to obtain insight into the roles and responsibilities of key stakeholders in organisational cyber security. We used a combination of the keywords and their derivatives:

“cyber security,” “information security”, “responsibility”, and “ownership” AND “accountability” AND “CISO” OR “Board” OR “Executive”. We also searched for issues and gaps identified in prior research to substantiate the need for this study. This literature review discusses the critical limits and gaps identified in prior research.

5.7 Premises

The arguments presented in this paper are based on the core premise of ‘Executives’ failure to understand and strategically value cyber security and the CISO prevents a unified approach to cyber security and widens the gap in achieving cyber corporate governance. As stated in our Phase 1 paper (nwfr), the underlying premises on which this research is based are as follows.

Premises # 1 to 5

1. Cyber security needs to be a business issue and fixed into corporate governance.
2. Cyber OAR must provide an algorithm for day-to-day managerial decision-making.
3. Cyber security as a corporate governance must be led by the highest-level executive.
4. Strategic cyber value must be steered by the expert in cyber security, the CISO.
5. CEO-CISO-OAR relationship is absent in organisational cyber corporate governance.

5.8 Results

Corporate governance dictates that “(1) authority, responsibility and control flows ‘downwards’” and “(2) accountability flows ‘upwards’” (Fenwick, McCahery & Vermeulen 2019, p. 179). We believe accountability also needs to flow ‘downwards’ and that executive accountability should be transparent to all other stakeholders. This is a strategic and operational gap in corporate governance and organisational cyber security that is not often met.

The strategic and operational challenges of cyber security that we raise here must be addressed before organisations can develop the cyber corporate governance framework needed to support cyber leaders to bridge the gaps identified (see Introduction) and the gaps between control requirements, technical issues, and business risks (Bakari et al. 2007, p. 45).

5.9 Participants’ demographics

Between January and March 2020, we conducted semi-structured interviews and gained rich qualitative data from 31 senior leaders and managers responsible for their organisation’s information and cyber security (Figure 5.1).

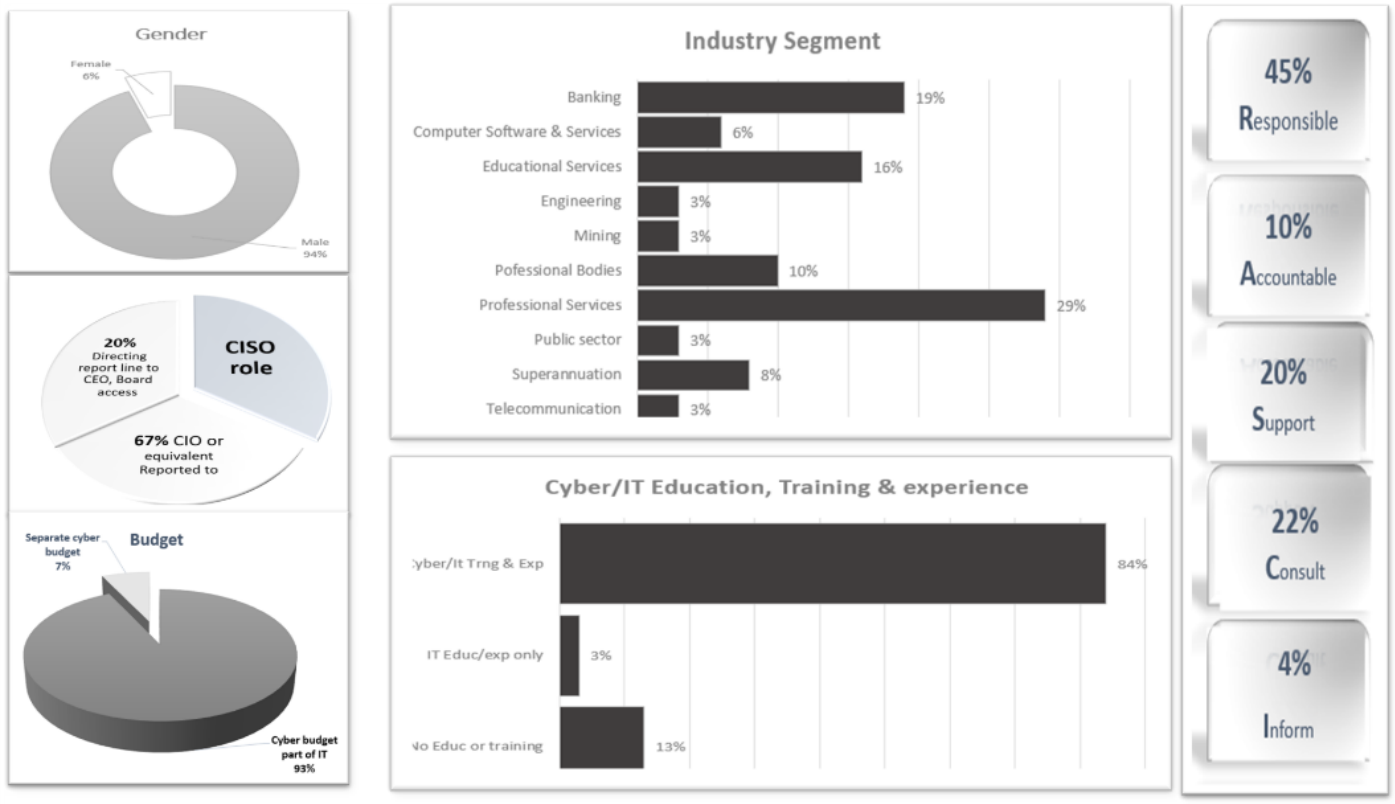

Figure 5.1. Demographic profile of participants

All participants had a lead role or responsibility in their organisation's information and cyber security. Although unacceptable, the gender composition of 6% women compared to 94% men in our study was expected. Cyber security remains a male dominated field where women represent 10% of the cyber workforce with 1% holding an executive management role in the Asia-Pacific (Stark 2017).

Of the study participants,16% identified as an 'accountable person' for end-to-end management and cyber security decisions; 45% believed they were directly responsible for developing the strategy and framework for cyber security (including the communication plan, training and awareness program, security operations and compliance).

However, 93% of those participants confirmed that the cyber budget (including resources) comes out of the CIO budget, in which they had no say. In job role and reporting line, 67% of the CISOs report directly to the CIO, 20% had direct access to the CEO and Board, and the remaining 13% were ambiguously placed. In terms of education, 84% stated they were IT educated and experienced, and have had cyber security training. The remaining 16% had a variety of disciplinary and educational backgrounds and levels of experience.

We restricted our research to the finance sector. The most significant representation was from the financial services industry at 56%, which (Figure 5.1) 19% banking and 8% superannuation. The longest bar in the chart shows participants from professional services (cyber consultants, predominantly accountants), specifically the 'Big 4' accounting firms which have become a

dominant force in the cyber advisory domain, with over 57% of their client base in the Financial sector. The other cyber industry segments interviewed comprised 16% educational services, 10% professional industry bodies, 6% cyber software services and finally, telecommunication, mining, engineering, and government at 3% each.

5.10 Participants' observations

Analysis and synthesis of participant observations indicated consensus among participants on most issues. We present findings that dominated across all data for each central issue. In this paper, we use pseudonyms for participants' anonymity.

5.10.1 Perceived role of the CISO

Most participants perceived the CISO role as ambiguous and awkwardly placed with responsibility without authority. They commented that although the CISO should be informing strategy their recommendations are usually disregarded or reduced to simple operational decisions at best. Two critical needs expressed were bridging the gap between the CEO and CISO as well as the role of the CISO to be extended as a trusted strategic advisor to the CEO, and the CEO to emerge as a promoter, sponsor, and advocate of cyber security.

5.10.2 Perceived role of CEO

All participants perceived the CEO as the leader in charge of setting and driving vision, purpose, and culture and directing the organisation's narrative (Dawson

2017). They agreed that a higher degree of cyber security compliance and uptake is needed at all levels and that it has to be driven – or at least sponsored – from the top. Otherwise, lack of executive commitment, endorsement, and oversight “would be setting us up for failure” (Ben).

Cultural alignment was seen as important:

> The CEO can directly influence the culture of the board and the senior executive; beyond that, the CEO’s cultural influence pretty much dies – unless every single direct-reporting person under these managers is a carbon copy of the CEO's culture (Joe).

Most participants commented that executives need to “play a more critical and active role” (Jayden) but that adopting such a strategy in practice has been slow. Participants noted that some executives are responding to new regulations such as CPS 234 but continue to view cyber risk as “just another risk measured as a compliance issue”. “The focus on cyber risk is often *ad hoc*” or only looked at “when something bad has happened – as opposed to being part of normal strategy” (Belle).

> Executives want to know it's all good, they want to get some form of confidence that it’s ok, but they don't want the detail because it's not always good to know what's going on (Tom).

Participants blame some executives’ lack of cyber awareness and misperception of risk and urgency for their disconnect from cyber security. Other executives see cyber security as a business risk, but ‘too hard’ or are put-off by the

“technobabble” and would rather pay for the risk to be managed. Participants noted that risk should be tracked as cyber opportunity and elevated to the wider corporate risk register.

Two-thirds of participants perceived that most executives ‘don’t know, don't care, don't understand’ cyber security value, and consider it ‘someone else’s problem’. They commented, however, that the introduction of new regulations is changing this, along with increased awareness of potential adverse personal impact.

Participants recognised that configuring good cyber security practices requires executives fulfilling their required cyber-OAR, and that organisational maturity affects measuring cyber-OAR readiness and capability but that “it is too often left up to the IT guy with no processes, no controls nor governance” (James).

Several noted that some cyber leadership issues (or immunity from the issues) could be sector-specific.

> Executives in the mining sector have a unique proposition, as many of those executives often come from an engineering background with knowledge in both technology and cyber security, and thus can address this critical issue from the ground up (Steve).

5.10.3 The emerging executive role

A striking observation was that executives must evolve as cyber-aware leaders as it is dangerous for cyber security responsibility to still sit solely with IT, but “most executives wouldn't even know where to start” (Tony).

Several participants recognised that exceptional cyber-aware leaders have emerged but have been a rarity. A common view was that “every single senior executive should understand cyber risk, and the importance of cyber security and cyber resilience – at least in general terms” (Joe). Although not executives or members of “strategic” leadership in their organisation, many referred to the strategic nature of key decisions in cyber security. “It should be a business-driven decision starting by understanding the risk in business terms” (Tony).

Several participants considered CEOs and Boards to be ignorant of their ‘crown jewels’ and their responsibility for them. Alternatively, CEOs and Boards were aware of these responsibilities but were unwilling to accept them. One CISO stated that Executive responsibility was about developing corporate KPIs that can be used as powerful tools to shift responsibility.

Many specified that the role of the Executive should be to support a partnership between cyber security, business, and IT. Participants largely agreed that cyber security is a board-level issue that existing governance mechanisms ignore. There was consensus that “cyber security continues to be seen as an IT issue, not a business risk”.

> This ignorance or lack of awareness is further propped up by the top consulting firms such as the Big 4 and [2]MBB that continue to produce

[2] Big 4 refers to four major Accounting Consulting Firms: MBB - refers to three major Management consulting firms

> reports from a cyber risk context, yet the organisational strategy perspective is absent from the complete picture (Belle).

Some participants commented that organisations continue to focus on siloed and unconnected internal workings, rather than viewing the organisation as a complex ecosystem. One participant argued that while the majority of board members in the top 200 ASX listed companies (less than 1% of GDP) are beginning to ask questions about cyber risk, this is uncommon.

One senior advisor observed that organisations may initiate cyber security programs, but executives are choosing to outsource due to their lack of understanding and awareness. Outsourcing provides a sense of reassurance for the concerned executive, but cyber-knowledgeable leaders consider using tick-box-behaviour outsourcing to be a pretence that leads to the false belief that by “paying for the top-shelf cyber solution, the risk has been managed” (Belle).

According to most respondents, executives continue to make assumptions about how they should treat cyber risk, presuming that:

> the attackers don't know who I am, so they're not going to come after me. If I can’t see them, then [they can't see me and] I can't be attacked (Belle).

This approach is often referred to as ‘security by obscurity’ and is infamous for not working. Belle went on to state that executives need to go a step further to manage the risk and look at it as a cyber opportunity.

Participants acknowledged that misapprehensions about and complexity of cyber security issues make dealing with and communicating those issues more challenging than other more straightforward workplace problems.

> Strictly speaking, cyber security is everyone's responsibility, the same as workplace health and safety (WHS). I use the WHS example "If you have a cable sticking out of the wall that's not been terminated, everyone in that workplace knows you should call your manager and then get someone to fix it because I don't want someone to get electrocuted" (Aidan).

Aidan stated that he believed this ownership of common responsibility does not transfer to cyber security practices.

Most participants emphasised that the CEO must drive cyber security transformation culture to avoid the scenario of people doing whatever they want. A common perspective was that cyber security needs to be fast-tracked and taken seriously at the executive level rather than merely paying lip service to it. Many asserted the Executive is critical to elevating, advocating, and promoting cyber security and its agenda to the Board, the C-suite, and the whole organisation.

5.10.4 Role and responsibilities of the CISO

Most participants interviewed were CISOs or worked with CISOs and commented that their views about the CISO role and responsibilities are common throughout their networks across different industries.

Participants considered that the previously invisible and silent CISO role is becoming more prevalent and visible and “fuelling controversies about where responsibility for data security ultimately lies within the organization.” (Kovsky 2019, p. 1). Unfortunately, the role is still undefined (Tokar 2020), which makes it difficult to promote the work and role.

Non-CISO participants made similar observations with a broader view. One professional (information security) consultant engaging with a wide range of clients stated.

> We find that there are still organisations without a CISO. For example, we started engaging with large financial organisations that did not have a CISO – the cyber security function was buried under general IT or the governance's team and pushed onto a manager (James).

Another commented the CISO “often do[es] not have the right level of power to get something done” (Nathan), which negatively impacts “the CISO’s ability to perform” (Seeholzer 2015, p. 91).

A recurrent theme was that CISOs are “just a glorified title; and treated as a glorified systems administrator with no authority, budget, or resources” (Geoff). Most CISOs expressed frustration, but only a small number were also resentful, and none believed that cyber security is “just IT”.

Participants reported emerging changes where CISOs are evolving into leadership positions and directly reporting to the CIO. Most expressed awareness of the need for cyber security to be strategic, holistic, and embedded with an

equal focus on resilience as on hygiene. Several stated that many CISOs now focus on developing and implementing cyber security strategy and are moving away from the traditional security role of first-line defenders. These participants noted that regulators are pushing for organisations to “demonstrate a dedicated cyber security function” (Geoff). The common response of the CISOs was to take up this challenge to be more strategic and to lead their leaders.

A view echoed across a number of participants was that:

> Cyber security is one of those things – when it works, you don't know – right? It’s not like you get points or you keep your job – because the organisation has not been breached (Aidan).

One CISO indicated a need to use business indicators to convey the work of the CISO.

> We prevented [countless] breaches, had eight hackers from Ukraine trying to access our firewall, but we blocked all of them. That way, the business sees the value on what they’re spending – otherwise, ‘it’s not working’ (Aidan).

Most expressed the view that cyber security must not be siloed. Each participant stated that to breakdown silos, the challenge is to inspire change and help executives grasp the importance of cyber security. Martin described the need to acknowledge that cyber security is more about “the culture, the engagement, the people side, the change side, the strategic alignment”.

A common theme raised was that the CISO's narrative needs to change from one of scare tactics to a cohesive story of custom-built and business-led cyber risk

strategy. The majority acknowledged that the onus is on the CISOs to manage upwards, build relationships, and raise awareness through education and reducing complexity. This involves ensuring the Board and executives be engaged throughout the process to make informed decisions together. However, they recognised that even when CISOs take up this challenge, there is no guarantee the Executive will respond appropriately.

Participants generally agreed that managing up is about raising cyber security awareness by speaking to business leaders and changing the cyber security narrative from an operational necessity to a top-level strategic priority (Martin) and shifting cyber security to a standard item on the Board's agenda rather than something talked about once-a-year (Steve) or when something goes wrong.

Many agreed that it is difficult to ‘sell’ security capabilities that are often seen as foreign or alien – and therefore frightening. Some who have awareness of personally identifiable information (PII) and no ability to protect their own online presence have trust issues arising from the fear engendered by IT capabilities:

> … the cyber guy is someone who ‘knows a lot of stuff’ so there are trust issues. They [executives] believe that you [the cyber professional] have a dossier on them (Brian, CISO).

5.10.5 The CISO as a strategic trusted advisor

Participants unanimously agreed that the CISO should be a strategic position, yet the CISO held a strategic-level role in only two participant organisations. Most participants asserted that cyber security needs to be separate from IT and the

CISO moved to a position reporting directly to executive leadership. The majority stated that despite the word “Chief” in their title, the role of CISO does not have C-suite status and lacks credibility.

5.10.6 Internal socio-political obstacles

The emerging socio-political obstacles, threats and weaknesses incorporated OAR principles, hierarchical structures, organisational culture and maturity, the lack of open communication and the role of HR. The most frequently raised topics were responsibility and accountability and question of “Who owns cyber security?”

Several respondents stated that, without authority, the demanding role of the CISO has an overreaching job description. Most considered that there has been slight but insufficient improvement since the introduction of the regulation CPS 234. This is due to regulations not being operationalised until the regulations are sufficiently detailed to be implemented and legislated (Tom).

5.10.7 Organisational culture

OAR was seen as the backbone of a cyber safe organisational culture. A consensus was that the missing link is the human and behavioural element. One participant argued that the issue “can’t be left to HR alone” (Tony) and that cyber professionals need to guide executives and help educate and build a cyber resilient culture. A common perspective was that the cyber roadmap should go beyond compliance (Sam) to include a well-defined strategy aligned and anchored into the corporate culture to execute a cultural change (Bryson) and

engage the “hearts and minds of our people” (Joe). Respondents argued that cyber culture needs to be continuously monitored. Failure to do so entrenches silos and groupthink that ignore cyber security measures (Jayne 2020).

A few participants suggested that different interactive mechanisms such as internal social media, posters, cyber campaigns and even incentives (e.g., winning an iPad) to complete training are needed (Andrew). Most stated that the concept of a cyber culture is slowly emerging but will take time. Several recommended an integrated organisation-wide culture of security that rewards good behaviour and reprimands bad behaviour to create a culture where everybody understands their individual role in keeping the organisation safe. Most believe that cultural change needs to be driven and backed by the Executive.

5.10.8 Communication

It was broadly agreed that while organisational culture is built on and supported by a sound communication strategy, communication is the biggest challenge impacting cyber security. Over two-thirds of respondents noted a common sentiment held across boardrooms is that cyber security is a steep learning curve and that the ‘technobabble’ is too challenging to understand. Participants expressed concerns that a ‘gloom and doom’ disaster narrative is widespread and points to a need to translate cyber security into a language the business community understands and that can be engaged in prioritising cyber initiatives.

A predominant view was that businesses care about two things – making money and saving money. Most believe a common language is necessary to reduce the ambiguity. Using the right words for the right audience with a relatable focus (e.g., money) is also important.

5.10.9 Organisation structure and maturity

A common concept raised was that structure impacts both communication strategy and culture. A pervasive concern was the adverse impact of organisational structure on the CISO's status, power, and authority when placed low in the hierarchy. Several participants stated they found themselves with a variety of inappropriate tasks and responsibilities in relation to their title.

According to many, undefined cyber workflows, and lack of communication plans or hierarchical value, have negative impact on the cyber maturity level. This is evident when contrasting organisational maturity in other domains against maturity in cyber security, that cyber security approaches and measures are inadequate. For example, large financial institutions have a good level of maturity within their own heavily-regulated responsibilities: “They have big capability and they have been making investments for years" (Peter). Mining is a sector where “cyber security is in line with safety and environment – and needs to be – as mining is comprised of a quite complex orchestration of activities that interact in real-time” (Steve). Where protected IP is vital to a domain (e.g., patents or geological samples) and where privacy and confidentiality needs are high (e.g., government-citizen databases), cyber security maturity tends to reflect the investment in privacy and protection.

Uncertainty in expressing maturity was common, as “there is no real measurement or metrics to demonstrate maturity or improvement” (Anton). Steps toward maturity include “understanding our risk profile and current level of maturity” (Peter), “reviewing and uplifting existing policies and even write new procedures” (James), “reducing the risk of exposure” (Peter), and “raising awareness and providing training programs and promotional campaigns” (Bryson) and not just “Do you tick this box?” (Tom)."

5.10.10 HR as an internal weakness

Participants reported that HR does not generally play a supportive role in cyber security and, in some cases, even has a prohibitive role acting as gatekeeper rather than enabler. Most participants suggested that research is needed to understand the key role HR plays in cyber security. Although the role of HR emerged as a critical component of healthy organisational cyber security, HR is addressed in subsequent papers and is not a focus of this paper.

5.11 Discussion

The dominant finding from our research is that cyber security is a leadership issue, and one that is complex and not easily resolved.

The complex sub-issues of cyber security leadership include the perceived and actual roles of the Executive and the CISO and the socio-political obstacles in OAR principles: hierarchical structures, organisational culture, and maturity. Cyber security remains a highly sensitive and contentious issue – undefined, debatable, and highly controversial.

Considering the need for cyber security to combat organisational risk, the failure to comprehend cyber resilience is worrisome. The severe chasm between what is truly needed for an organisation to be cyber secure and cyber resilient, combined with prevailing perceptions and behaviours, leave organisations vulnerable. This chasm is compounded by the dangerously weak strategic positioning of cyber security which must be rectified if there is to be healthy development in organisational cyber security.

The CEO and CISO roles present a chicken-and-egg conundrum: which comes first? Does the CEO step up and take on the cyber-OAR (despite not having requisite knowledge and expertise) and place their trust in a CISO they probably don't know well (and who is unlikely to have the business management experience or strategic insight)? Or does the CISO step out in faith – at risk of being fired – to educate and enable the CEO as a 'cyber-newbie' while simultaneously learning business and strategic leadership principles themselves? Each of these two ventures is both necessary and a high-risk undertaking. For either CEO or CISO to take such a momentous step if the other does not, is hazardous both personally and organisationally, with no guarantee of success. In fact, if only one of the two takes the risk without the other, there is a greater likelihood of endangering organisational security than the current, very undesirable situation.

With this dilemma in mind, we discuss the ramifications of our findings.

5.11.1 CEO and CISO roles and responsibility

The need to define expectations of the CISO role and how the CISO fits into the bigger picture of organisational cyber security is essential. However, there are vital foundations to be laid first. One foundation is to resolve the misconceptions that cyber security is an IT issue and cyber risk only a tick-a-box exercise. Without a belief in and commitment to cyber security as vital, the Executive will not be able to undertake the desperately needed cyber leadership and OAR of their organisation and will not be open to the CISO attempting strategic cyber security.

During our study, we observed a shift in which (persuaded by new regulations such as CPS 234) executives have begun to show interest rather than seeing it as ‘someone else’s problem’. This is an excellent start but is insufficient. Our claim that ‘a belief in and commitment to cyber security is vital to organisational wellbeing’ – a supposition both easier and harder than many of our other recommendations – is another necessity. This foundation requires no new knowledge, expertise, or skills. It requires a change of attitude.

Once committed, the natural subsequent actions will then be dictated by the Executive’s own drive. The ensuing activities will of necessity include new knowledge, expertise, and skills and most notably the development of a trust-based relationship with the CISO.

The CISO also needs to make difficult changes. For some it means a change of mindset and recognising the need to step up to a strategic business role. There is

also the formidable challenge to (trust the Executive and) speak out, step up, and risk being a ‘newbie’ in business-thinking, lexicon, and strategic decision-making in a field where executives are used to being the expert. These two opposite dilemmas are essentially the same. For both CEO and CISO, the ‘formidable challenge’ is risking personal image – in their own eyes as well as others’ – by taking on the role of a learner within their role of ‘expert’. This is the crux of the crisis. Without the fear of losing face or losing control, the people involved would be much more open to the needs of cyber security.

Longstanding socio-political obstacles have introduced further complexity to bridging the gap between the CISO and Executive. Beyond the absence of trust, these include resolving OAR, rigid structures, unsupportive culture, low-level maturity, poor communication, and weakness of HR. Each obstacle needs to be dismantled or overcome, but none can be successfully tackled until both the Executive and CISO have adapted their mindset as recommended.

5.11.2 Increasing resilience through trust

Absence of trust is a fundamental aspect of the ‘formidable challenges’ of mindset change and building a partnership between the CISO and the Executive.

Trust provides critical-to-business benefits including collaboration of ideas and actions which aid in removing silos. Silos and fragmentation are prevalent and damaging and anathema to trust. Cyber reform requires a trust-enabled vision that filters into day-to-day operations engrained into the culture.

A premise of cyber resilience is that an organisation **will be** successfully attacked at some point and that business continuity **must be** maintained when this occurs. Cyber resilience is a combination of strategically planned preventative, corrective, and proactive measures with backups, Plan B, and built-in readiness, all of which require a bedrock of trust and cooperation.

Whether considering basic cyber hygiene or comprehensive cyber resilience, trust is the cornerstone that determines the strength of the entire structure.

5.11.3 Ownership, accountability, and responsibility (OAR)

Our second dominant issue is resolving the cyber-OAR. Cyber security needs to be a CISO-and-CEO-partnership in which the CEO holds final ownership, accountability, and responsibility (OAR).

The CISO must be given the power, authority, and budget requisite to meet their responsibilities. The executive must accept and acknowledge – privately and publicly – that in cyber security, ‘the buck stops here’. These tandem needs return us to our primary argument for a trusting, strategic partnership between the CEO and CISO.

These roles – even in partnership – are not identical. Legally, ultimate OAR resides with the Executive, but the CISO’s knowledge, expertise, skills, experience, and networks require they exercise their cyber-OAR capabilities in partnership with their CEO. Consequently, the CEO and CISO must trust each other and work together strategically to meet the cyber-OAR needs.

Future cyber-OAR must be embedded in corporate governance. Organisations must first establish a cyber strategic plan and roadmap, publicly asserting Executive commitment. Every delegated responsibility must be clearly assigned with appropriate authority; cyber security role definitions, from CISO to intern, must specify relevant authority to meet responsibility. Cyber security experts must be empowered to collaborate with the Executive so that cyber objectives can be implemented and, eventually, aspire to cyber corporate governance.

5.11.4 Adapting the organisational structure

Cyber security is a complex strategic and operational problem, and rigid structures lack the flexibility and agility needed to be resilient in a rapidly changing digital environment. Information drives strategy and decisions, and protecting the confidentiality, integrity, and availability (CIA) of an organisation's information is critical to strategic, operational, fiscal, and practical ability to thrive or survive. When information assets are distributed throughout all aspects, departments, procedures, and processes of the organisation, and information is a generated product and by-product of everything done by everyone in an organisation, traditional hierarchical structures are detrimental. The silos and fragmentation inherent to rigid structures are also detrimental and prohibitive to resilience.

Rigidity is a catalyst to inadequate reporting, ineffective communication, obscured authority, and confusing workflows. Flexible, agile structures require trust, and well-developed OAR to enable embedded CIA and resilience; a

requirement that restates our foundation of strategic and mutually trusting leadership.

5.11.5 Cultivating culture fit

Culture is tightly tied to both structure and leadership. Every organisation has its own unique (non-transferable) culture expressed and manifested through behaviours, customs, and collective practices. A combination of executive attitude and CISO silence has created an unsupportive culture, often reflected in uncaring or mindless tick-a-box compliance. The common attitude ‘if the bosses don’t care, I’ll do what I want’ creates an obstructive and unhealthy culture.

Our study found that many organisations with an otherwise healthy or productive culture exhibited poor cyber culture. Although irrational, this misalignment of attitude and approach to cyber security is often overlooked in otherwise well-run organisations.

Again, this issue is based on, and can only be improved by, foundations of trust, and integrity of strategic leadership that demonstrably practice what they preach.

5.11.6 The role of HR

The HR department – whether human resources, human relations, or human well-being – plays a critical role in managing and maintaining organisational culture. HR’s directive to delineate policy (and consequences) that protect the organisation from misbehaviour and irregularities, and their responsibility for recruiting, training, and replacing personnel, makes HR gatekeepers. HR’s resultant power plays a key role – positive or negative – in cyber-culture. As this

paper is focussed on the CEO and the CISO, the HR role in cyber security is out of scope and left for future research.

5.11.7 Developing cyber maturity

With organisations at different stages of the maturity scale, there is no ‘one-size-fits-all’ solution. To attain cyber maturity, an organisation needs a strategic program that is business-led and resilience-focused. A cyber maturity program must connect with both strategy and day-to-day operations.

Cyber maturity integrates all three aspects of cyber security: the people, processes, and technology. For a strategic program to protect and mitigate against foreseeable, known threats and unknown emerging risks, a proactive approach including raising cyber awareness, integrating cyber into the culture, and aligning and merging cyber risk with business risk, is required. Executive support, buy-in, and example are essential. Cyber resilience requires cyber security be baked in, not merely bolted on.

5.11.8 The role of communication

Communication is a key enabler of cyber security and its biggest challenge. Cyber experts must be able to translate security language into a language of business enablement. CISOs can overcome misperceptions by avoiding alienating hyperbole and scare tactics. Instead, business language and key business indicators such as ‘return on investment’ (ROI) and ‘cost-benefit relationship’ (of cyber resilience) to the ‘bottom line’ communicate the integral role and value cyber security provides.

Executives also need to master a second language. A dominant finding is the parallel between cyber risk and other key business risks such as fiscal and legal risk. If executives use familiar risk management lexicon, they should be able to intelligently discuss themes such as cyber-risk appetite, cyber-strategy, cyber-controls, cyber-resources, cyber-investment, and so forth. Taking time to listen, ask questions and comprehend, will enable the executive to start a conversation with the internal cyber-team.

Improved communication intersects with other critical issues such as cyber-awareness and communication and will remove the cacophony of multi-origin terminologies. It will also help build and embed trust and shared understanding and improve engagement.

5.12 Limitations and future research

This paper presents findings from a qualitative exploratory study. Inherently, limitations include the necessary parameters. Data was gathered from 31 participants – a large sample from a qualitative perspective, but still limited. We restricted our investigation to the finance sector. We are therefore unable to claim generalisability, although we can potentially claim transferability. Finally, our research scope was limited to large corporations, so research is needed to explore the issue for small-to-medium organisations.

This article reports on Phase 2 of a 3-phase study. Future research to conclude this study will explore all the issues discussed here, draw on theoretical lenses, and develop models to illustrate and further explore our findings to date.

5.13 Conclusion

When we set out to investigate the contemporary and practical problem of organisational cyber security leadership the solution seemed as simple as bridging the gap between the CISO and the Executive (CEO and the board). A chicken and egg conundrum emerged that clearly indicated both of these roles needed to change in a unified effort to bridge the gap.

As we delved deeper into our empirical data, socio-political obstacles emerged. These newly identified gaps uncovered a bigger and challenging problem. The key mechanisms of corporate governance are needed to promote the shared stewardship approach required.

We concluded that, as well as the relationship between CISO and CEO, changes are needed in the organisation's governance. Neither the CEO nor the CISO can effectively resolve organisational cyber-OAR issues in isolation. Nor can the OAR of organisational cyber security be resolved consecutively. Ideally, CISO and CEO must work on cyber-OAR simultaneously **and** in partnership.

We have built the argument that these core issues combined underlie current ongoing problems with effective organisational cyber security. When viewed together, instead of in isolation, they cohere to form the basic description of an organisational cyber security ecosystem. We conclude therefore, that the aspirational future state of organisational cyber security will see a more united and resilient cyber leadership approach where the CISO is transformed into a strategic and trusted partner to the CEO; together, the CEO and CISO can form a

united vision and build capabilities that support the aspirational future goal of a strong cyber resilient organisation. Cyber security and cyber resilience will become embedded in organisational corporate governance.

CHAPTER 6: Phase 3

6.1.1 Brief Introduction to Phase 3

This Chapter 6 is the third and final of the three papers, reporting on Phase 3.

Highlights

- Cyber security needs to be embedded in corporate governance.
- Cyber and business ecosystem silos must merge as one ecosystem.
- Cyber security governance must be led by the highest-level executive.
- CISO must play an active role as a trusted-strategic advisor in cyber governance.
- Resilience needs cyber governance ecosystem led by committed strategic leadership.

The reference for this manuscript is:

> Psaroulis, G., Jerram, C., (forthcoming) “Cyber corporate governance ecosystem – the aspirational future state”, (submitted to Journal of Strategic Information Systems).

6.2 : Paper 3: Statement of Authorship

Statement of Authorship

Title of Paper	The aspirational future state of cybersecurity: A cyber corporate governance ecosystem
Publication Status	☐ Published ☐ Accepted for Publication ☒ Submitted for Publication ☐ Unpublished and Unsubmitted work written in manuscript style
Publication Details	Psaroulis, G., Jerram, C., (forthcoming) The aspirational future state of cybersecurity: A cyber corporate governance ecosystem, (submitted to Journal of Strategic Information Systems)

Principal Author

Name of Principal Author (Candidate)	Georgia Psaroulis		
Contribution to the Paper	This paper was co-authored, but all the initial foundational work, including premises, questions, research objectives, interviews, analysis, and models, are my original work.		
Overall percentage (%)	65 %		
Certification:	This paper reports on original research I conducted during the period of my Higher Degree by Research candidature and is not subject to any obligations or contractual agreements with a third party that would constrain its inclusion in this thesis. I am the primary author of this paper.		
Signature		Date	24/01/2022

Co-Author Contributions

By signing the Statement of Authorship, each author certifies that:

i. the candidate's stated contribution to the publication is accurate (as detailed above);

ii. permission is granted for the candidate in include the publication in the thesis; and

iii. the sum of all co-author contributions is equal to 100% less the candidate's stated contribution.

Name of Co-Author	Cate Jerram, PhD		
Contribution to the Paper	Major contribution is to writing, wording, and editing. Support in development of concepts and ideas (most original ideas and concepts are Georgia's original work).		
Signature		Date	03 Feb 2022

Name of Co-Author	no further authors		
Contribution to the Paper			
Signature		Date	

Please cut and paste additional co-author panels here as required.

6.3 Abstract

This paper presents the third phase of a six-year study into organisational cyber security leadership. A multidisciplinary scoping review in Phase 1, followed by a tightly focussed literature review and qualitative empirical exploration in Phase 2, provided the foundations for the synthesis and theoretical exploration of our findings in Phase 3. Dominant theoretical lenses are triple-loop learning theory for Phase 3 building on Stakeholder theory which has been the theoretical foundation for the entire study. A series of models illustrate our findings. Conclusions confirm our premise that organisational cyber resilience requires committed strategic leadership that provides an embedded holistic cyber corporate governance ecosystem.

Keywords: Cyber security, corporate governance. governance mechanisms, Ecosystems, Executive (CEO and Board); Chief Information Security Officer (CISO).

6.4 Introduction

This paper presents Phase 3 of a study on organisational cyber security leadership. This research is built on a comprehensive scoping review which was completed in Phase 2. Scoping encompassed a highly-focussed review and empirical investigation into the complex issues identified in Phase 1. We found that Ownership, Accountability and Responsibility (OAR) and the roles and relationships of the Executive and the CISO accounted for the predominant problems facing organisational cyber security today. This third study applies theoretical lenses to examine and challenge our findings and develop models to illustrate our results.

This paper explores our findings, including claims that ill-defined OAR and CISO job descriptions often lead to inadequate cyber security, poor cyber culture and non-strategic decisions that impede organisations from achieving cyber resilience. These issues are detailed in Research Design. The objective of this research and this paper is to build a case for an aspirational future state of cyber security by means of developing a “cyber corporate governance ecosystem”.

Our approach emphasises the *strategic* importance of cyber security in organisations. It offers an aspirational goal to develop a cyber corporate governance ecosystem that embeds cyber resilience into the daily health and wellbeing of the organisation. This study commenced in late 2017 to explore the impact of leadership on organisational cyber risk management and resilience.

The thesis for our study is that the future health and wellbeing of organisations requires not only best practice cyber security (protection and defence) but also cyber *resilience* – the ability to bounce back, survive and thrive after a successful cyber-attack. This aspirational future state of organisational resilience calls for cyber security to be a strategic business support activity with an end-to-end view of enterprise-wide processes. Beyond operational practices, cyber security (including resilience) must be embedded as an ecosystem – ideally, a 'cyber corporate governance ecosystem'.

6.5 Material and methods

Despite compelling contributions in top-quintile journals from high profile thought leaders and experts, integrating cyber security into the corporate governance ecosystem has made little progress. To contribute to this neglected and under researched issue, we conducted a multi-year multidisciplinary study of corporate cyber leadership.

This third phase primarily focusses on applying theoretical lenses to challenge and verify our earlier findings. We summarise the design and methods of the three-stage study then substantiate our central claim that a 'cyber corporate governance ecosystem' does not yet exist. Finally, we assert the potential for an aspirational future state and discuss what is needed to achieve it.

Theoretical drivers, theories and methodologies employed throughout our study are described. Next, we explore the principal issues of leadership approaches to organisational cyber security through three distinct phases – React, Reframe,

and Reinvent. Finally, we consolidate our body of work as a ‘whole picture’ and propose moves towards the aspirational goal of a cyber corporate governance ecosystem.

6.6 Research design

This study used a three-phase, predominantly qualitative, approach.

Summary Phase 1. Scoping review. We conducted an exploratory scoping study drawing from several scholarly disciplines better to understand this intricate and complex problem. The resultant rich information generated new explanations and potential areas for new research (Tisdale 2016).

Summary Phase 2. Focussed review and empirical study. This phase focussed on real-world perceptual insight gained from leaders, security specialists and cyber professionals.

Summary Phase 3. Refined synthesis and theoretical construct. Combining results from the first two phases allowed us to explore and synthesise our findings. We then developed models to depict the current state of organisational cyber security and a potential aspirational future state.

6.6.1 Phase 1: Scoping review

The scoping review from Phase 1 has been published in detail in (nwfr). This review of the research identified gaps across multiple disciplines to effectively address strategic leadership and the role of (non-IT) leadership in organisational cyber security.

Exploring leadership as a core issue at the heart of cyber domain problems resulted in a rapid escalation of the scale and scope of the Phase 1 review. Cyber security is still in its infancy as an academic discipline. Indeed, cyber security is not recognised as a complex multidiscipline separate from IT or computer science. Our scoping review drew upon insights from a broad range of contributing disciplines. Although each discipline had some relevant input, on the whole there was a dearth of quality academic publications causing a heavy reliance on grey literature. We used stakeholder theory to guide our questions to ensure focus and relevance.

The scoping review results provided a comprehensive list of interrelated themes and patterns of thought and behaviour in organisational cyber security. This insight led us to develop tentative models of the current state of organisational cyber security and a potential aspirational future state (nwfr).

The themes, patterns and tentative models arising from Appendix B formed the basis for and shaped the research and interview questions of Appendix E.

6.6.2 Phase 2: Focussed review and empirical study

The empirical study has been published in (nwfr). In-depth semi-structured interview questions were formulated from the Phase 1 scoping review. They were designed to explore the complex issue of cyber leadership by gaining practice-oriented insight on how this role is defined, determined, and enacted in organisations. Again, stakeholder theory was employed.

We recruited 31 participants and assigned each a unique pseudonym. After transcription and data-cleansing of interviews, the respondents' demographics were categorised. The responses were then analysed through a series of coding passes. The first pass identified patterns and determined common themes. These were then refined to a few supra-codes identified by an iterative synthesis of patterns, core categories and unique themes discussed in our second research paper (nwfr).

6.6.3 Phase 3: Refined synthesis and theoretical construct

In our first paper (nwfr) the detailed scoping review highlighted the siloed, fragmented, and multidisciplinary nature of the current practice (Appendix A). One of the significant findings was the absence of corporate governance in organisational cyber security and the absence of the cyber security in corporate governance. Here, we revisit, refine, and investigate our scoping review.

Sources for Phase 3 focussed on the themes relevant to the concept of a "cyber security corporate governance ecosystem", using the following five databases (1) ABI/INFORM Collection; (2) Business Source Ultimate; (3) Scopus; (4) Google Scholar and (5) Google. We chose these databases for quality and coverage of high-quality content. Using the advanced search, we conducted a more thorough search using a combination of the following keywords and subsets "cyber security", "information security", "corporate governance", "ecosystem" and "environment". The limited and dated results provided further imperative, as the scarcity of current or even recent literature strongly indicated the need for research in this field.

We further narrowed our search parameters to focus solely on peer-reviewed journals and found 30 peer-reviewed articles across seven specific disciplines (

Table A. 6 in Appendix I). A qualitative coding exercise employing the keywords to interpret and identify the overarching themes, further refined the search. For preliminary results and more search details, see Table A. 8(Appendix I).The literature indicated that both praxis and academic theory need these issues explored, and drove the method, propositions, and shape of this research.

6.7 Theoretical constructs

The driving objective was to explore leadership in organisational cyber security as a complex, interconnected, multi-level and multidiscipline construct. We identified multiple significant issues, most of which are the concern of corporate governance. We then identified that the theme or approach of a ‘cyber security corporate governance ecosystem’ had not previously been explored as a single conceptual framework. We searched for prior research contributions and gaps (Appendix I) and confirmed the scarcity of quality publications relating to ‘cyber security corporate governance ecosystems’.

The “multi-” nature of this concern directed us to consider theoretical constructs that enabled us to synthesise the breadth and focus of the issues. The theoretical constructs we discuss here encompass the identified components and themes of cyber security, cyber corporate governance ecosystems, and theories drawn from other disciplines.

6.7.1 Finding the constructs

Our focussed search (Table A. 5 in Appendix I) identified only 30 relevant articles that used the terms “cyber security”, “corporate governance”, and “ecosystem”, only one of which mentioned *all three* concepts. That article (Daud, Rasiah, George, Asirvatham & Thangiah 2018) established three major themes that underscore the need for our research.

Theme 1 is a need for a clear and direct relationship between corporate governance and cyber security. Theme 2 is the need for top management support and commitment based on recognition that cyber security responsibility requires the highest Executive-level to define, set and achieve organisational security objectives. Theme 3 stipulates that management and the organisation need to recognise that their cyber routine operations do not work in isolation and are not detached from its ecosystem; on the contrary, they need to adopt a collective and cooperative approach across all levels of the organisation, including their external associations.

We reassert, as reported in Paper 1 about our study (nwfr), that cyber security will remain fragmented and siloed if these three issues are not addressed (Daud et al. 2018).

6.7.2 Refining the question

Our premise is that true cyber security incorporates cyber **resilience** as well as cyber hygiene and protective measures and is a complex, interconnected, multi-level and multidisciplinary construct. To explore the legitimacy of this premise, we

deconstruct the core underlying concepts to frame the questions to be addressed. Through Phase 1 (scoping review) and Phase 2 (focussed review and empirical research), we refined the concepts used to drive Phase 3 of the study. They are:

1. Cyber security must be embedded in strategy and corporate governance.
2. Cyber security corporate governance must be led by the highest-level Executive.
3. The business ecosystem and cyber ecosystem must be incorporated and considered holistically, at both strategic and operational levels.
4. The Executive must elevate their CISOs to a strategic role and empower them to fulfil their responsibilities.
5. A cyber security corporate governance ecosystem as a single conceptual framework has not previously been explored.

6.7.3 Cyber security and corporate governance

“Corporate governance remains an exigent task” (Adnan & Ahmed 2019, p. 12). The current siloed and fragmented cyber security is a patchwork of efforts with little or no alignment to corporate governance (Kuerbis & Badiei 2017). Hence “cyberspace governance remains a complex problem” (Peng 2018, p. 469), in which organisations “fail to contain firm-level [cyber] risks before they become systemic risks” (Li 2014, p. 267).

Information security (infosec) – including cyber security – is a core and integral component of corporate governance. Von Solms (2006, p. 165) refers to

corporate governance as the ‘crucial’ Fourth Wave after technical (1), policy management (2), and standards and best practice (3) and makes it clear that each wave progresses the maturity of cyber security. With the aid of Solms' fourth (IS governance) wave, our analysis found that current reactive cyber practices sit very low on the maturity scale, confirming the need for cyber corporate governance.

The traditional stand-alone governance approach of cyber security does not work. Cyber security needs to be a permanent item on the Board’s agenda (Mishra 2015) and embedded into the organisation’s overall corporate governance program (Da Veiga & Eloff 2007). This has not yet transposed into practice. Some recent shifts recognise cyber security as a collective and co-operative concept from management downwards, including external relationships. However, any application reported has been described as disconnected, inconsistent, and patchy (Daud et al. 2018).

While there have been research efforts to develop corporate security governance guidelines and frameworks, little is known about a business ecosystem-wide approach to cyber governance.

6.7.4 Executive responsibility

Cyber security has rarely reached the Board. However, due to the new regulations, it is now added (somewhat) to the agenda, albeit seldom with understanding or commitment. A sentiment echoed by many of the participants in our study was:

> Security is not regarded as being an issue apart from they [referring to Executive management] understand it has to be … it's not on their radar. Until something goes wrong (IT manager cited in Maynard, Tan, Ahmad & Ruighaver 2018, p. 75).

Consequently, the approach to cyber security governance practices is *ad hoc*, fragmented, and unplanned and exhibits a "lack of even the simplest accountability processes" (Maynard et al. 2018, p. 67).

Traditionally, risk management responsibility has fallen squarely on the shoulders of the Executive (CEO and Board). **Cyber** risk demonstrably falls into the category of corporate risk management (Maynard et al. 2018) and therefore corporate governance. Despite Executive reluctance, a consensus is gradually forming on the need for corporate governance and strategic direction for cyber security.

Executives must learn to perceive "cybersecurity as strategic rather than operational and as an opportunity rather than an expense" (Hepfer & Powell 2020, p. 41). Such an approach requires a fundamental mindset change to enable management to view cyber security as valuable rather than expensive.

Infosec governance is a plan–do–control–measure–report loop that starts with (1) management's commitment, sanctioned by policy and approved by the Board to (2) develop a suitable organisational structure specifying (3) ownership and the breakdown of responsibilities to all levels. The loop closes with (4) feedback to top management of current risk status (Von Solms 2006, p. 167). The often

neglected fourth step of feedback is important. Once the cyber strategy is set, even at an operational level, it “does not preclude the need for Executive-level management support” (Maynard et al. 2018, p. 167).

It is evident in the (sparse) literature, that cyberspace is a corporate governance responsibility (Von Solms & Von Solms 2018) but understanding how executives can protect their respective companies in cyberspace requires further research (Da Veiga & Eloff 2007).

Our research shows that executives do not have a good understanding or knowledge of cyber security and lack the training and/or motivation to do so. It is, therefore, essential to acknowledge that, though a broad issue, cyber security is the CEO’s responsibility (Von Solms & Von Solms 2006). Where executives lack the understanding and knowledge to promote cyber security to its strategic status, we find that cyber security and its governance remain outside the realms of corporate governance.

6.7.5 Corporate governance ecosystem

Cyber risk extends beyond organisational boundaries but as cyber security is generally not included as part of corporate governance, the broader cyber ecosystem has not really been attended to (Daud et al. 2018).

“Cybersecurity is an ecosystem comprised of multidisciplinary, multi-layered activities and qualities, the components of which are interrelated” (Tisdale 2016, p. 209), cannot be separated from other business functions (p. 88) and requires Executive-level management interventions (p. 4).

Too frequently, cyber security is viewed in isolation as external to the wider business ecosystem. Both strategic and operational cyber security approaches and practices must ensure that cyber security is embedded throughout the organisation and its extended value chain. To accomplish this, executives must understand how cyber risk interweaves throughout the organisation's complex business ecosystem.

This understanding is fundamental to the ability to direct change and guide the organisation's direction to ensure it is robust, resilient and maintains key elements of value (Moore 1993). An ecosystem perspective focusses on the alignment of various actors (Adnan 2016) and their cooperative or collaborative behaviours (Nambisan 2018). This shift requires that authority and control be distributed (Adnan & Ahmed 2019) end-to-end over the entire business ecosystem.

A fundamental tenet of corporate governance is that a strategic framework must address the human component – the key actors in the cyberspace ecosystem (Peng 2018, p. 465). Ecosystems are inherently designed to connect people and be open (Rattray, Gijsbers, Tikk, Purdy, Mulvenon & Carr 2011). They require a holistic perspective based on a people-orientated approach (Da Veiga & Eloff 2007).

Cyber security is never secure unless all stakeholders are committed, so stakeholders – particularly employees – must have a voice in the corporate governance Fourth Wave Loop (Von Solms 2006). Good relationships with customers, suppliers, business partners and even competitors (Hepfer & Powell

2020) need to be developed as part of the whole ecosystem (Da Veiga & Eloff 2007) if the organisation is to be secure.

6.7.6 The Chief Information Security Officer (CISO)

Our literature search revealed a disturbing absence of references to the CISO and their role in cyber leadership, governance, or the ecosystem. Although the CISO is often solely responsible for cyber security, if employed in an operational role they should not be held responsible for strategic governance. Lack of respect for the CISO's role, and failure to recognise the challenging work they accomplish without authority or budget, is cause for concern.

6.8 Theoretical influences

6.8.1 Triple-loop Learning theory

The multidisciplinary nature of cyber security posed a particular challenge to our research. Filtered through the lenses of Stakeholder theory (Freeman, Wicks & Parmar 2004) and Triple-Loop Learning (TLL) theory (Tosey, Visser & Saunders 2011), we drew on a broad range of contributing disciplines, approaches, and insights that helped us shape, build and structure a theory specific to our vision of cyber security as a multidiscipline.

This paper introduces TLL as the dominant and overarching theory used for synthesising our analysis which had drawn upon understanding provided by stakeholder theory and other contributing theories, such as institutional and upper echelons theories (Figure 6.1).

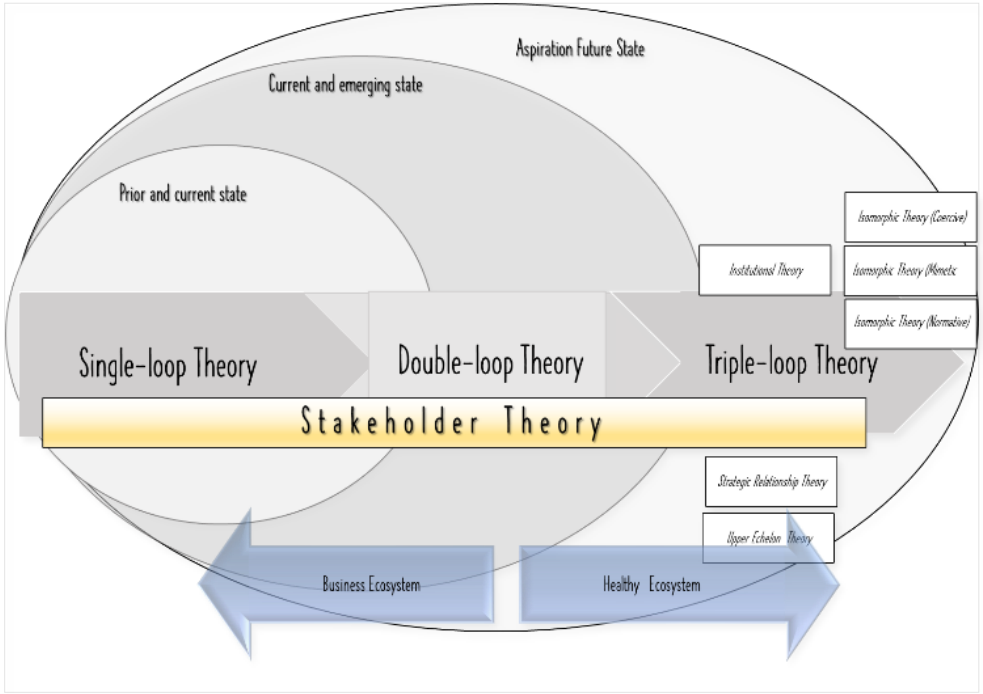

Figure 6.1. Theoretical influences

Literature about business ecosystem health became a critical component of, and foundation for, a comprehensive and integrated theory-base for a cyber corporate governance ecosystem. The theories' application in our analysis and subsequent synthesis are discussed in Principal Issues.

Organisational learning refers to the process by which "organizations gain experiences, undergo failures, and learn to survive" (Lee, Hwang & Moon 2020, p. 366). TLL theory analyses the quality of organisations' responses to failure and the degree of learning and therefore the quality of their survival and wellbeing. We posit that genuine cyber security and resilience require a triple-loop learning level response to risk and experience.

"Argyris (1976) asserted that the learning process in an organization is not a one-time phenomenon but rather one that happens through multiple loops or iterations" (Lee, et al. 2020, p. 366). Such a shift would entail "meaningful change in process, structures, assumptions or concerns" (Snell & Chak 1998, p. 341) hence altering the inner workings of the organisation's ecosystem.

It is not an organisation, but the individuals supported by a healthy workplace that solves the problems and produces the behaviour that leads to learning (McClory, Read & Labib 2017, p. 56). This referring to employees *and* executives, has only recently been adopted by many in the cyber security arena. This is a position exemplified in the stubbornly human practice of silos and territorialism which are strongly indicative of single-loop learning in an organisation.

The siloed and fragmented nature of organisational cyber security is particularly dangerous. Each of the fragmented silos is an important part – but only a part – of a complex multidimensional problem that needs all of its components to work together. Collaboration across silos requires at least a double-loop learning approach.

A critical aspect of the complex problem of organisational cyber security is the leadership and the question of who has ownership, accountability, and responsibility (OAR). We have framed the current dilemma of problematic OAR and leadership as a ‘cyber governance paradox’ that poses a severe risk to the business, its day-to-day operations, and long-term survival and wellbeing. This dilemma is compounded by the fact that most organisational leaders are insensible and therefore take no or limited corrective action.

We attribute this insensibility to the notion that many executives feel overwhelmed by the unfamiliarity, ambiguity, and uncertainty of cyber security. It requires courage to step beyond a single-loop learning approach in areas of confidence; it is much more challenging in unfamiliar territory such as cyber security. Even progressing to double-loop learning requires courage and commitment.

Creating a cyber corporate governance ecosystem requires not just double but triple-loop learning. TLL refers to three progressive levels of organisational learning (Seo 2003). Level one, single-loop learning, refers to instrumental actions in which learning is reactive and singularly applied to each problem each time. Using single-loop learning, organisations take corrective action to get back

on track without questioning or altering underlying practices to achieve the desired outcome (Labib 2016; Lappi, Lee & Aaltonen 2017).

Double-loop learning (DLL) is a deeper level in which driving values are challenged and developed. Applying DLL involves reflection and reframing, questioning assumptions and correcting the contextual rules and norms underlying action and behaviour (Weishäupl, Yasasin & Schryen 2015).

TLL is about learning itself (Massingham, Massingham & Dumay 2019), and challenges even more deeply than double-loop learning the assumptions, values, mindsets, and core beliefs that underlie policies, decisions, and purpose.

Single-loop learning (SLL) asks, ‘Is this right?’ and seeks to fix; double-loop asks, ‘Am I doing this right?’ and considers fixing the process; triple-loop learning asks, ‘What is right?’ and works to embed values (Aston 2020; Massingham et al. 2019).

TLL involves trying to ascertain how we make decisions that frame our work principles and pursue a goal and/or aspiration (Tosey 2005). TLL is the desired level of investment to achieve both a healthy and a cyber resilient organisation; however, applying triple-loop learning can “have unintended consequences” and “requires profound organizational unlearning” (Tosey et al. 2011, p. 302). Checks and balances are necessary to protect the organisation as active triple-loop learning impacts the entire ecosystem and revolutionises the organisation’s ethos (Tosey et al. 2011).

6.9 Other theoretical influences

6.9.1 Stakeholder foundation

Stakeholder theory was the foundation theory for analysis in our earlier phases of this research. A stakeholder is any “group or individual who can affect or is affected by the achievement of the organisation’s objectives" (Hörisch, Freeman & Schaltegger 2014, p. 329).

We use the refined Stakeholder and Strategic Relationship theory in Phase 3 for its focus on building and promoting a value-laden approach (Davis 2017) to corporate governance; it refers to knowing how to engage the inner circle to gain support, buy-in and commitment (Freeman, Phillips & Sisodia 2018).

As presented in Paper 1 (nwfr), the cyber domain has a broad group of stakeholders with different roles, all pushing their own agenda and dialogue to influence organisational cyber security strategy. Yet little is known about managing multiple stakeholders’ relationships and the heterogeneous nature of their many demands (Bundy, Vogel & Zachary 2017, p. 496). Strategic alliances, partnerships, and networking will effectively foster cooperation, building trust and achieving value congruence and strategic complementarity within critical relationships (Bundy et al. 2017) between cyber stakeholders.

6.9.2 Institutional and related theories

Cyber security is unpredictable. Its increasingly volatile environment sees significant disruption to the organisation’s day-to-day activities. The theoretical

lens of institutional theory and related concepts gives some insight into current organisational practice.

Phrasing the present dilemma as being “stuck in an isomorphic institutional rut or path that has consumed its structures, processes and culture, norms, and, in the long run, its organisational goals” (Caravella 2011, p. 3) is an insight gained through this lens. This perception allows us to see the factors that limit the ability to change and develop new structures, and therefore inhibit the change needed to achieve our aspirational future state.

Key stakeholders can influence and pressure organisational practice towards isomorphism using subtle coercive, mimetic, and normative social processes (Caravella 2011, p. 5). Such pressure pushes for conformity, and specifies the profession and paths required to ‘gain legitimacy’.

This isomorphic path of inertia, persistence and conformity inhibits the ability to adapt and change; it prevents the organisation and its leaders from successfully differentiating organisational features including operational policies, administrative arrangements, and tactics. These are all vital elements in achieving any aspirational future state of organisational cyber security governance ecosystem.

6.9.3 Upper echelons theory

Upper echelons theory (Hambrick 2007) studies top executives and their effects on strategy and performance. We claim cyber security must be embedded in corporate governance and led by the upper echelon. Therefore, executives and

their biases and dispositions determine the existence, shape, and effectiveness of any cyber security or resilience in their organisation.

“Executives view their situations – opportunities, threats, alternatives, and likelihoods of various outcomes – through their own highly personalised lenses” (Hudson 2018, p. 1). An informationally complex domain such as cyber security that deals with critical but uncertain situations is not objectively “knowable” but merely interpretable (Kay & Goldspink 2015). This is disconcerting to executives responsible for leadership in a discipline in which they are (usually) uninformed and have little or no experience.

As cyber security and resilience are very much a strategic executive domain issue, the willingness and ability of the Executive to become strategic leaders in this strange new domain is vital to their organisation’s survival and wellbeing.

6.9.4 Business ecosystem

Organisations do not exist in isolation. Rather, they coexist in digital, interconnected, dynamic, complex business ecosystems (Moore 1993). They are “a network of participants, a governance system, and a shared logic” (Thomas & Autio 2014, p. 1).

Building a business ecosystem requires rethinking business boundaries and traditional corporate ownership structures and borders. The business ecosystem comprises complex connections and interrelationships between heterogeneous actors who play different complementary roles.

Community is a fundamental aspect of the ecosystem concept that allows collaborative individuals to share in creating and delivering a specific value proposition (desired solutions) in a dynamic changing climate. The combination of individuals in the community, freedom of creativity, and encouragement to question tradition and values in the organisation maintain and promotes the ecosystem's overall health. This can only be led by the Executive.

6.10 Principal issues

In this paper, we limit ourselves to discussing only the principal issues from our study. The work presented in this paper builds upon foundations laid in our two previous papers (nwfr).

6.11 Principle Issue 1: React – single-loop learning

In our first research paper (nwfr), we reported on a multidisciplinary scoping review that led us to develop the cyber governance paradox model depicting the not-yet-ecosystem. This model (Figure 6.2) shows the key stakeholders and how these individual stakeholders potentially influence organisational cyber security. It also depicts each stakeholder's relationship to the overall process.

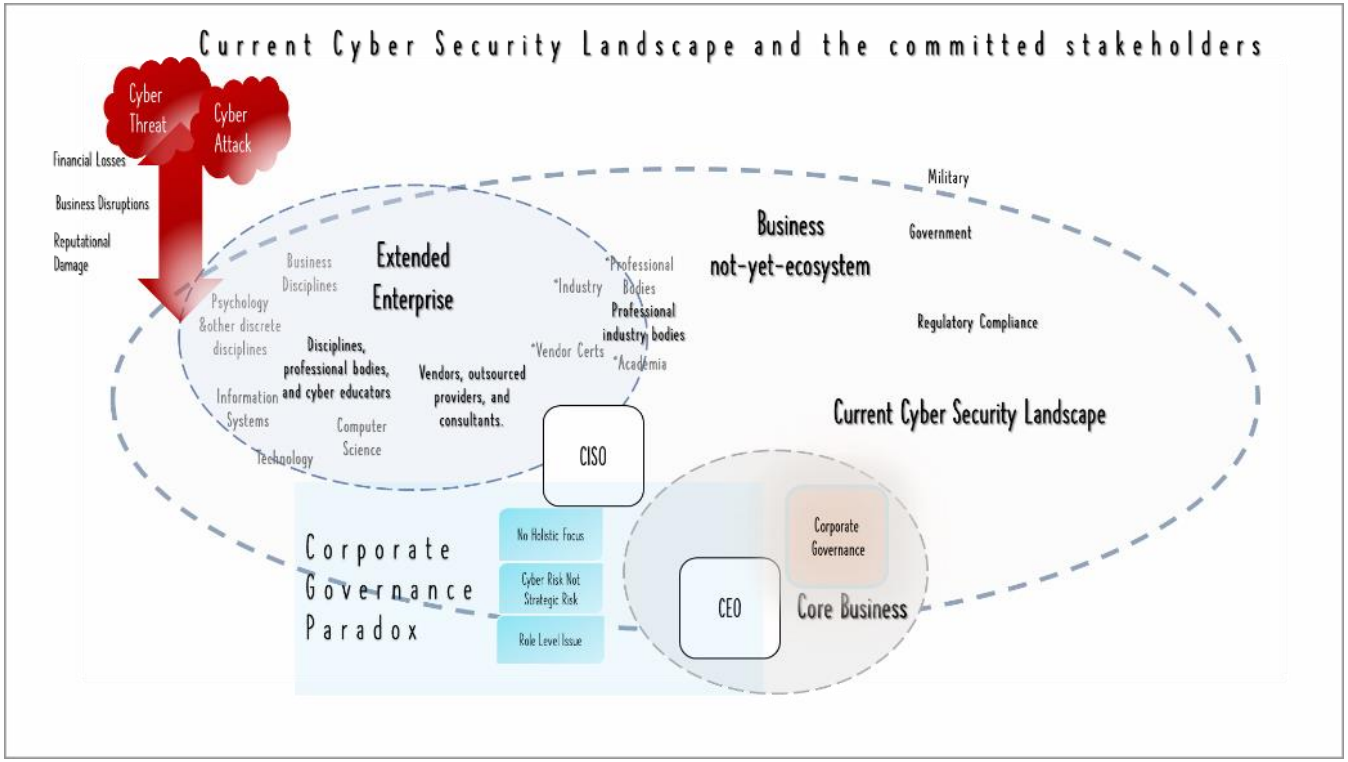

Figure 6.2. Phase 1: Cyber governance paradox: not-yet-ecosystem

Ideally, the organisation's cyber security domain would be an ecosystem. As the current landscape is siloed and fragmented, it would be inaccurate to label it as a system, let alone an ecosystem. We therefore present our concept of an aspirational cyber corporate governance ecosystem and refer to the domain in its current state as a "not-yet-ecosystem".

6.11.1 Cyber governance paradox model

The inner circle in Figure 6.2 represents the core business, the outer circle represents the extended enterprise, and the organisation and its leaders' expanding circle describes the area in which relevant but unconnected stakeholders engage in-apposite activities. The large oval circle with broken lines depicts the expanding circle of the business not-yet-ecosystem incorporating two key stakeholder groups: the government and regulators.

Governments (allied with the military) are recognised leaders in cyber security and together, with the quasi-governmental regulators, are viewed as powerful actors in the domain. Although they play a vital role to lead and guiding toward better security and resilience, they are rarely in close association or in partnership with organisations other than defence contractors.

6.11.2 The extended enterprise

Vendors, outsourced providers and cyber consultants, cyber education providers, and professional bodies are dispersed and often committed members of the extended enterprise (Figure 6.2, outer circle not-yet-ecosystem). Each member

plays a key role – independently – in the domain of organisational cyber security. IT vendors and outsourced providers can be inextricably linked to the business through Managed Service Agreements but have a different agenda and are more focussed on selling isolated proprietary lock-in software than on the organisation's best long-term cyber resilience profile.

Professional bodies and cyber education providers also coexist independently. They offer training, professional development and certification accreditation and other important benefits. Nevertheless, they maintain autonomy and legitimise the profession through normative forces mapped to their own policies. These policies enact and enforce the ideas, norms, and language expected of their members rather than those of the client's organisation, its culture, or strategic objective.

6.11.3 The CISO

The CISO is the subject-matter expert focussed on IT and IS security compliance yet has strange and uncomfortable placement in the outer circle (Figure 6.2), set apart from the core business as the CISO role (usually) lacks status, power, and authority and has restricted access to the Executive with no voice or autonomy. Ramifications of this placement are many and significant and are the focus of our second paper (nwfr).

Isolated from the strategic inner circle and deprived of power or budget, a CISO relegated to the outer circle can only make technically driven piecemeal decisions. One of the repercussions of this placement is it deprives the CEO of a

strategic, trusted cyber-subject-matter expert. Instead, the Executive is dependent on a fragmentation of advisors from different silos (e.g., Technology or Finance) who provide disparate bits of agenda-biased information which will often conflict with or obscure the actual expert information provided by the undervalued non-executive CISO.

Two of our major themes coalesce in these circumstances: excluding the CISO from the inner circle and strategic planning is risky; siloism further diminishes the CISO's status and ability to perform.

6.11.4 The core business

The inner circle (Figure 6.2 core business layer) consists of the Executive (CEO and Board) acting in a "soloist" keystone and orchestrator role for cyber security. The model also depicts (shadowed, in dotted lines) the not-yet-existent emergent silhouette of cyber corporate governance. Although currently non-existent or still in infancy, it is represented on the model as a needed (emergent) fundamental aspect of organisational cyber security.

6.11.5 Cyber governance paradox: The Executive

The Executive needs to take the lead role in harmonising this complex domain to mediate stand-offs, negotiate trade-offs, and resolve conflicts to maintain balance and develop cohesion across this diverse group of stakeholders. This issue is problematic as so many executives, with limited and selective perception, see cyber security as such a low priority they fail to grasp why urgent action is required to protect and defend their organisation. The failure to act further

aggravates organisational risk as those unwilling to invest strategically in defence are even more unwilling to invest in resilience. Such leadership leaves the organisation extremely vulnerable to increasingly common cyber-attacks, and almost guarantees an inability to recover from a successful attack.

Cyber corporate governance is a core attribute of security and resilience. Lack of cyber corporate governance causes many issues that hamper organisational cyber security. This is the “cyber governance paradox”. If leadership remains reactive and embedded in defensive single-loop learning, even when complying with regulatory demands, the CISO does not have the necessary strategic weight to compensate. We illustrate this in Figure 6.3.

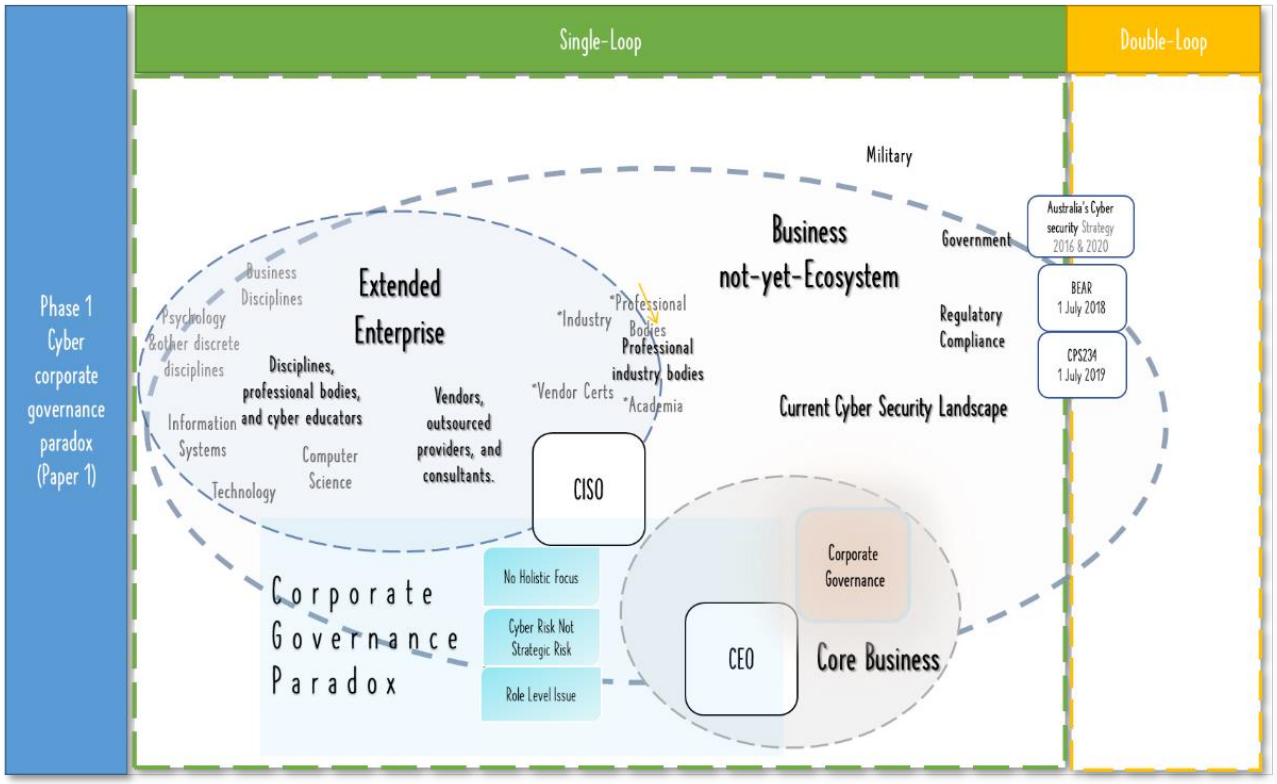

Figure 6.3. Cyber governance paradox: single-loop learning

6.11.6 Single-loop learning

SLL involves taking steps with set criteria to solve a problem, without concern for root causes (Figure 6.3). It therefore neglects to question underlying operational designs or causes. Such mindsets and habitual responses can include the sceptical “if/when a breach occurs” (Sadowski 2020, p. 1), the default abrogation to cyber technicians “to use their know how” (Salimath & Philip 2020, p. 478), or to mindlessly follow the organisation’s policy and procedure manual to fix the problem by “inserting code to fill in, or ‘patch’, a vulnerability” (SolarWinds n.d., p. 6). Unknowledgeable, habitual actions that default to a single-loop learning approach to address problems do not bring about a change to the status quo. The mindset that defaults to such thinking is also at the heart of unwillingness to venture more deeply into dealing with cyberspace.

Most organisations’ cyber security practice is stalled in the vicious cycle of single-loop learning. “Error-hostile” (Pfeiffer & Wehner 2012) organisations adopt a reactive firefighting find-and-fix approach that triggers a prolific number of technically focussed quick-fix solutions to cyber threats rather than looking at the real issues (Antonucci 2017; Edgar & Manz 2018).

Narrow perception of cyber security as “just IT” and relegation of responsibility without strategy or power to the CISO both lead to and cause organisations to become trapped in learning lock-ins and single-loop learning. This vicious cycle, single-loop learning approach prevents the necessary growth to address the

underlying design. The inadequate cyber security reinforces the underlying mindsets that cling to single-loop learning approaches.

The *sine qua non*-approach towards cyber security puts coercive pressure on the government to raise the level of cyber awareness and provide guidance. The Australian Government introduced Australia's Cyber Security Strategy 2016 after which Australian Prudential Regulation Authority (APRA) implemented new mandatory regulations BEAR (2018) and CPS234 (2019). These regulations mandate that the onus for cyber security is on the Executive. Although these changes are centred on uplifting the cyber sector and legitimising the practice, there has been limited or no collaboration across the larger cyber domain. This has led to slow uptake of these reforms (except when intersecting with GDPR and European clients or when large fines are levied).

This approach reinforces single-loop learning. A DLL approach (at least) is needed for cyber security leadership to build a strategic and holistic cyber security domain. DLL theory (Argyris 1977) teaches us that a prerequisite for such growth is the willingness to question the governing rules, mechanisms, and mindsets that the current practice. The 'cyber governance paradox' is a natural outcome of the *Reactive* approach of single-loop learning. Developing a double learning approach both requires and leads to a *Reframing* approach.

6.12 Principle Issue 2: Reframe – double-loop learning

We explore how a double-loop learning approach could lead to the gradual emergence of cyber security in the inner circle (Figure 6.4).

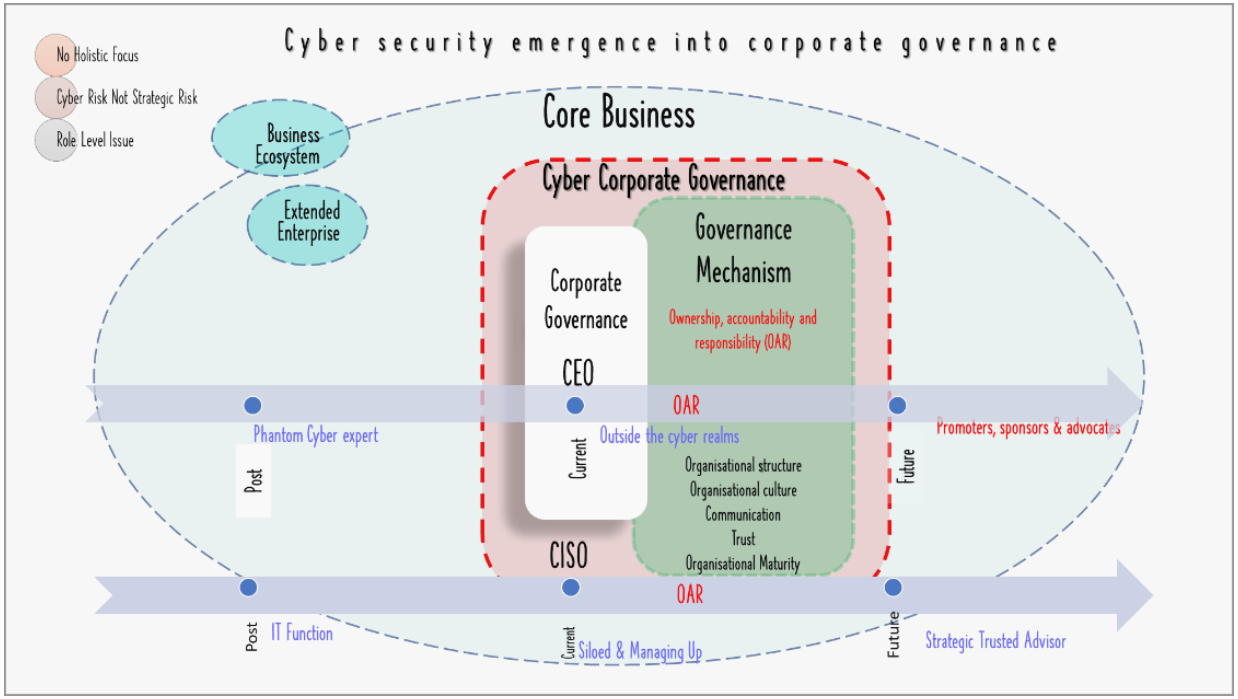

Figure 6.4. Phase 2: Cyber security emergence into core business

6.12.1 Core business and double-loop learning

Our model (Figure 6.4) focuses on core business, concentrating on corporate governance, governance mechanisms, the Executive and the CISO and their relationship. This model illustrates how double-loop learning could stimulate progress towards development of network partnerships, bridging silos and reducing fragmentation. Governance mechanisms required to develop maturity such as OAR, organisational structure, culture, communication, and trust are incorporated. Our empirical research suggests that in some cases these governance mechanisms are emerging.

Our model also hints at the need to progress to the not-yet-realised goal of triple-loop learning. Our research also suggested encouraging shifts in attitude where some CISOs are considered a trusted strategic advisor with CEOs becoming promoters, sponsors, and advocates of cyber security. Such progress, however, was limited to a minority.

6.12.2 The CISO

In our model (Figure 6.4), the CISO is represented on a continuum (lowest blue arrow). On the left, the CISO is positioned as a glorified title without requisite status, authority, or power, trying to manage up. The continuum moves to the right toward the aspirational state in which the CISO role evolves to an Executive position (infrequent and far from the norm).

The middle of the CISO continuum shows the results of double-loop learning in which the CISO becomes the business enabler. Our research participants emphasised that for this to occur, the CISO needs to 'change their narrative'. Language and story need to make the cyber work visible and the criticality apparent. When CISOs are able to master these lexicon and story changes, they will cease to be seen as alien or peripheral and gain credibility and support from the Executive.

The strategic and trusted CISO-as-advisor is exceptionally rare. Our empirical analysis showed this as a needed ideal positioning, but achieving this aspirational future state requires double or triple-loop learning mindsets. DLL, when genuine rather than superficial, allows some growth in each of the issues discussed but we find that application of double-loop learning in this domain varies substantially and is inconsistent.

6.12.3 The Executive

CEOs are also on a continuum (Figure 6.4, higher blue arrow). They are structurally positioned with ownership, expertise, and prestige with the Board (Haga, Huhtamäki & Sundvik 2021). They make or influence strategic decisions regarding corporate governance and its mechanisms. In our research, the CEO role emerged as a dominant theme and the model shows the slow but progressive changes of the CEO role from that of the phantom cyber executive (far left) to one that promotes, sponsors, and advocates cyber security initiatives (far right).

Generally, the CEO is the leader in charge of setting and driving vision, purpose, and culture and directing the organisation's narrative. We rely on CEOs who can leverage their transferable skills and abilities, personal knowledge, experience, and expertise to successfully lead the organisation. This is the norm. Unfortunately, as noted throughout this study, their limited personal knowledge, experience, and expertise in cyber security causes them to abrogate these attributes and responsibilities in cyber security. Consequently, CEOs (generally) fail to be the leader in charge of setting and driving vision, purpose, and culture and directing the organisation's narrative in cyber security. We have named this CEO role a 'phantom' cyber executive.

The CEO's role in the aspired future state is that of an executive who does play a critical role in elevating, advocating, and promoting cyber security and its agenda to the Board, the C-suite, and the whole organisation. Cyber security would be a new capability added to the CEO's valuable transferable skills.

6.12.4 Corporate governance

Even where general corporate governance is sound, corporate governance is significantly absent in cyber security or, equally important, cyber security is absent from corporate governance. Although corporate governance of cyber security is slowly evolving, it does not yet have a strong presence in most organisations (Figure 6.4, dotted lines corporate governance).

Governance mechanisms delineate the attributes needed in cyber security governance. These are represented centrally (Figure 6.4, also dotted lines)

overlapping corporate governance, with the CEO clearly central, and the CISO involved (but less responsible for the OAR than the Executive).

The important role of HR is not present in the models presented in this paper – but not because we do not value the role of HR. HR needs to be a knowledgeable partner in the recruitment, culture development and educational aspect of cyber corporate governance. Currently, HR participates in cyber security to different degrees and different purposes, most frequently to provide compliance training or to play a punitive role in cases of breach. Despite the vital importance of HR and its contribution to corporate governance of cyber, our models and discussion are confined to the focus of this paper.

Corporate governance, governance mechanisms, and all personnel in all roles, need to be considered in terms of application of double and triple-loop learning. As learning progresses from reactive to reframing, mindsets change and mature, and governance mechanisms alter in tone.

Although we are presenting a case for a triple-loop approach, it is unlikely that organisations (or people) with single-loop learning mindsets can leap to triple-loop learning approaches. We are therefore discussing progressive development from single- to double- then triple-loop learning mindsets and approaches to cyber security. In our model *Cyber security emergence into core business: double-loop learning* (Figure 6.5), we elaborate our model *Cyber security emergence into core business* Figure 6.4) with double-loop learning.

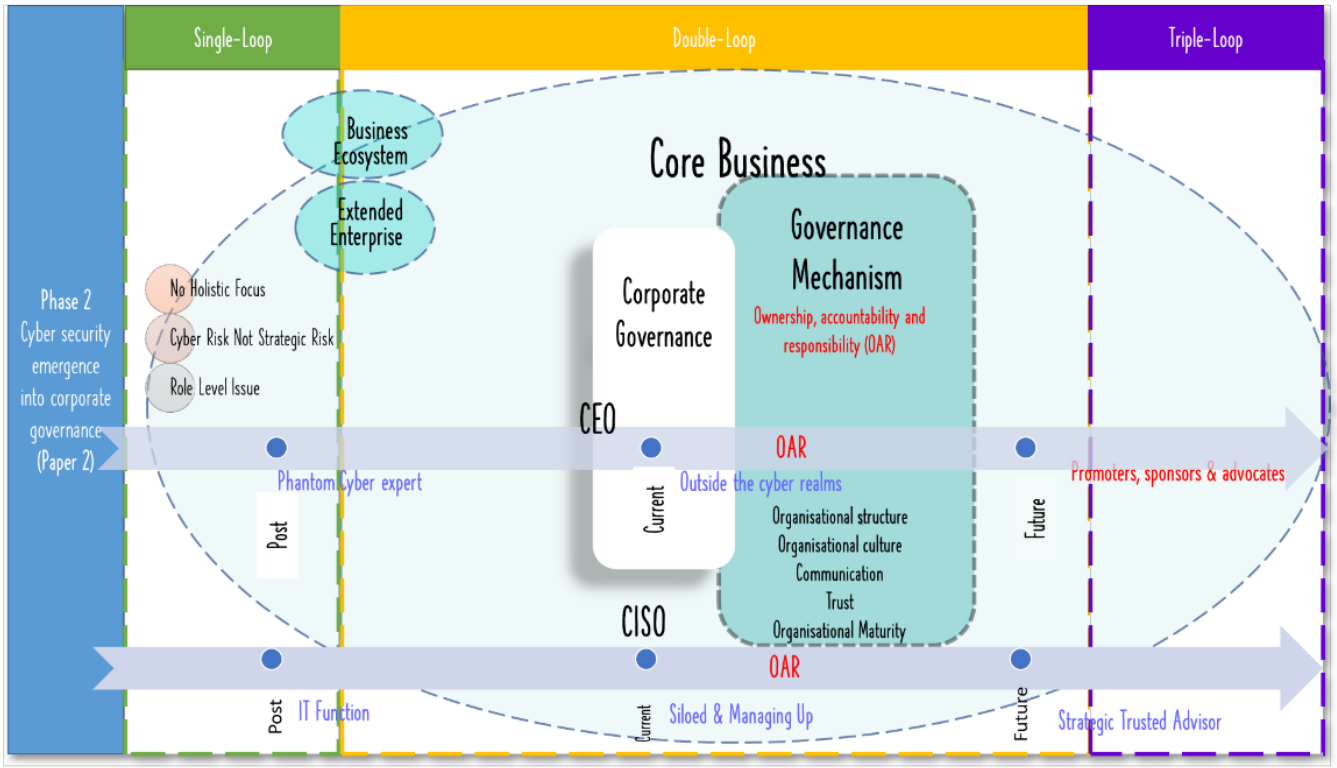

Figure 6.5. Cyber security emergence into core business: double-loop learning

Our model (Figure 6.5) is divided into three sections: single- double- and triple-loop learning. The CEO and the CISO continuums move from single-loop learning superficial cyber security (far left), through double-loop learning networked cyber security, and ideally towards aspirational triple-loop learning approaches (far right) that would generate a healthy cyber corporate governance ecosystem.

6.13 Principle Issue 3: Reinvent – triple-loop learning

TLL theory is the instrument used to synthesise our research findings. Our final model, *Cyber corporate governance ecosystem: triple-loop learning* (Figure 6.6) presents the aspirational future state of organisational cyber security as an ecosystem governed by coherent, unified, and committed leadership and stands in stark contrast to the current state depicted in our first model.

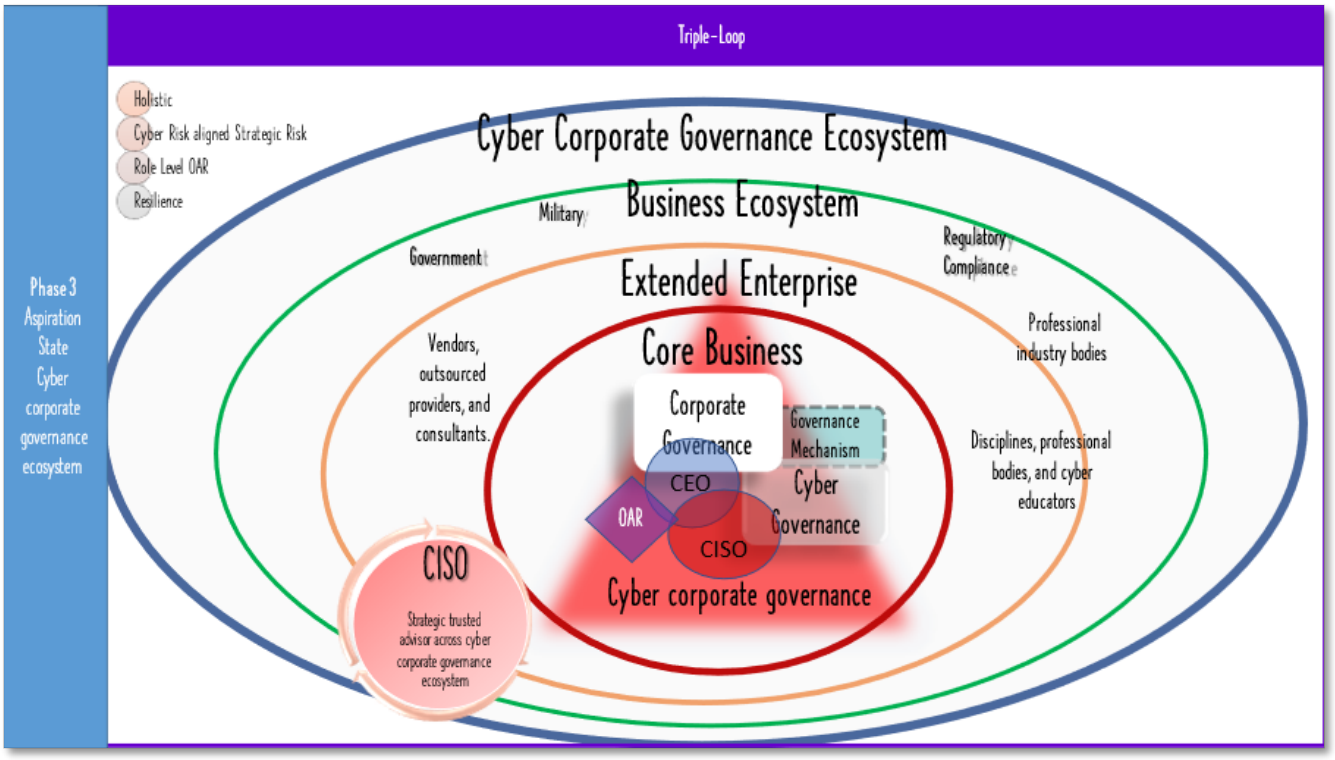

Figure 6.6.Cyber corporate governance ecosystem: triple-loop learning

6.13.1 Encircling the ecosystem and core business

In our aspirational model, organisational cyber security is seen to be a complex but coherent ecosystem. To deal with the complexity, the model depicts significant shifts in roles, relationships, and culture. We explore this from inside-out and outside-in.

Core business and the inner circle (red sphere) are now centrally placed as part of the broader community and culture of cyber security. Core business and the inner circle have changed to incorporate the desired partnership between CEO and CISO in strategic corporate governance. As our model is focussed only on cyber security, it does not incorporate all other members of the C-suite who also belong in the strategic inner circle of core business. Cyber corporate governance underlies all core business. General corporate governance and governance mechanisms, including cyber and cyber-OAR, are clearly profiled.

Each and all of our identified cyber stakeholders are placed in the concentric circles that portray the appropriate relationships and interrelationships required to enable a healthy cyber ecosystem. Core business and the inner circle are now surrounded by and therefore central to the extended enterprise (orange oval) of third parties, business ecosystem (green oval) and cyber corporate governance ecosystem (blue oval) protecting them all.

Third parties are now located for cyber as they are for other aspects of business in the extended enterprise. The placement of government and regulators again reflects the usual business relationship, located in the business ecosystem. Both

the extended enterprise and the business ecosystem reflect normal business operations and relationships – a “new” strategic positioning not standard in cyber practice today.

An unusual element in our model is that the CISO is represented twice: firmly positioned as a strategic trusted advisor in the inner circle; and separately located as an important influence and driver across the entire cyber corporate governance ecosystem with active involvement in each of the layers. The model is specific to cyber security and does not reflect other “normal” relationships; for example, the CEO is actively involved beyond the inner circle in many aspects of business.

The recognition of cyber security as fundamental and all-encompassing to any organisation that needs protection and resilience is a genuinely new element in this model (Figure 6.6). This necessitates the significant changes portrayed in the role of the CISO and the incorporation of cyber into corporate awareness, governance, relationships, and behaviour.

Each stakeholder group has a role to play, and each holds different levels of heightened influence (ALVA 2021) over organisational cyber security. It is not commonly known, but some relationships are already developed or developing and contributing toward the vision of cyber security as a comprehensive, multidisciplinary, business-embedded ecosystem. The Open Cybersecurity Alliance (OCA) project, established in 2019 by cyber security vendors such as IBM Security and McAfee, is a joint venture of like-minded cyber professionals and thought leaders who openly and collaboratively work to tear down cyber silos

(Tan 2020). They share best practices and promote advancement in the cyber security ecosystem. The AISA-ISC2 strategic partnership was formed in 2020 to strengthen, develop capability (ISC2 2020) and remove the current narrow technical scope.

These partnerships lead the way for organisations and executives interested in pursuing a new approach to cyber security. This kind of support is invaluable for developing double-loop learning and growing towards triple-loop learning.

6.13.2 Triple-loop learning

As stated in Theoretical Influences, TLL is about learning itself (Massingham et al. 2019). It is concerned with reflecting on *how* we best learn and *why* (Johannessen, Gerger Swartling, Wamsler, Andersson, Arran, Hernández Vivas & Stenström 2018). This enables continual improvement for individuals and their organisations. It requires even deeper shifts of mindset, thought, and behaviour than double-loop learning.

In our model (Figure 6.6), TLL is the frame (purple rectangle) and overarching framework. TLL is represented as an almost invisible but comprehensively pervasive and important foundation for the concepts presented. It develops and promotes collective mindfulness which is a natural outcome of a culture of triple-loop learning and has a salubrious effect on cyber awareness.

The aspirational future state requires drastically changing the underlying ideologies (Gupta, Briscoe & Hambrick 2018) of the organisation and its ecosystem. We need to consider and address problems (single-loop) but take

into account the deep underlying causes and contexts, (double-loop) then question the essential principles on which the organisation is based (triple-loop), impacting individual, interpersonal, and organisational levels, and their interrelatedness. Therefore, our ‘future state’ is about tackling (and probably re-inventing or co-inventing) the organisation’s identity and character – its ethos. Hence the aspirational goal of a cyber corporate governance ecosystem is developed and maintained through triple-loop learning and collective mindfulness.

6.14 The future state cyber security ecosystem (recommendation)

6.14.1 Leaving the fragmented and silo ecosystem behind

Traditionally, the domain of organisational cyber security has been hampered by the fragmentation and silos from and in which the disparate stakeholders operate. Individual cyber- and business-stakeholders must move beyond single-loop learning and put aside traditional siloes. Agreement on a new common lexicon must be built to enable effective communication so that a unified and strategic approach to cyber security can be possible. Although a degree of consultation has developed between some stakeholders (exhibiting a move towards double-loop learning), consultation has rarely extended to collaboration. Leadership and collaboration are key components in addressing siloes and fragmentation and laying a foundation towards effective and cohesive cyber security.

6.14.2 Redefining roles and relationships to OAR

Our research (Figure 6.2 to Figure 6.5) has revealed a lack of cyber-OAR and an inappropriate and unsupported strategic nature of the CISO position, despite the role's importance in organisational cyber security. Redefining the roles, as must occur for cyber corporate governance (Figure 6.6), requires that executives accept their OAR, step into genuine cyber leadership roles, and elevate the status of the CISO to one of trusted strategic advisor and partner. So too must CISOs be able to understand cyber security strategically and holistically.

CEOs, Board members and CISOs must therefore develop a double-loop learning approach (Figure 6.4) to enable growth towards triple-loop learning (Figure 6.6). They must collaborate to defeat silos, acknowledge the vital strategic role of cyber security, and develop a unified lexicon.

6.14.3 Understanding the need to protect organisations

The cyber governance paradox must cease to allow organisations to change and achieve future state cyber resilience. Executives must now accept and comprehensively act upon the critical strategic nature of cyber security.

The stimulation provided by regulatory pressure has triggered a degree of double-loop learning. However, lack of cyber security knowledge and expertise for many has impeded genuine double-loop learning. For instance, attempting to emulate what other organisations are doing to meet compliance is "transitory and superficial" (Argyris 1977, p. 121) and provides a false sense of legitimacy with questionable results.

Cyber resilience demands new strategic cyber security policies and practices designed in consultation with the CISO. Alternatively, any practices adopted from other organisations must be adapted and aligned to the organisation's unique mission and values to genuinely protect and safeguard their future.

6.14.4 Moving towards a corporate governance ecosystem

Our stated premise is that if an organisation wishes to build healthy cyber resilience, they need to nurture a cyber corporate governance ecosystem. First cyber security and resilience must be embedded in core strategy and integrated into strategic corporate governance. Second, cyber hygiene practices must be strengthened and built upon; strategic plans must be laid to build cyber resilience and ensure recovery after the almost inevitable successful cyber-attack or breach. Third, all independent (though complementary and synergistic) stakeholders must be engaged in co-opetition (Lappi 2017) as part of a healthy cyber ecosystem.

The nurturing process of laying the foundation must be iterative, a continual process of maintaining, monitoring, and growing the ecosystem. Key integrated components of the core strategy will require constant revisiting by the strategic leaders (CEO and Board in partnership with the CISO and other recognised cyber experts). Similarly, cyber-culture-building must be embedded and nurtured.

The partnership between the CEO as promoter, sponsor, and advocate of cyber security and the CISO as a trusted strategic advisor will set and drive vision, purpose, and culture and direct the organisation's narrative as a united front.

With this dual responsibility, both parties will acknowledge that – morally and legally – ultimate ownership and accountability reside with the Executive. The qualities required to attain this level of partnership, organisational growth, and cyber resilience are developed through triple-loop learning.

6.14.5 Ecosystem health

The success of the ecosystem “can be evaluated through its health” (Lappi et al. 2017, p. 28) at both the organisation and business ecosystem levels as well as at the cyber corporate governance level. Ecosystem health success is dependent on the dynamics of “resilience, sustainability, innovativeness, and renewal” (Lappi et al. 2017, p. 34). These and other critical attributes important to cyber security and to ecosystem health are attainable through triple-loop learning approaches.

6.15 Conclusion

We present a new approach to organisational cyber security and propose a shift from a high-risk fragmented organisational approach with an absence of clear and coherent leadership to the aspirational model of a unified Cyber corporate governance ecosystem. We demonstrate use of triple-loop learning theory for in-depth analysis of cyber security.

Our research supports our initial premise that a cyber security corporate governance ecosystem as a single conceptual framework has not previously been explored and that cyber security needs to be embedded in corporate governance. We have further demonstrated and modelled that the business

ecosystem and the cyber ecosystem need to be incorporated and considered holistically, at both strategic and operational levels. Cyber security corporate governance must be led by the highest-level Executive in the organisation. Equally, the CISO as strategic trusted advisor is a vital yet all-too-often absent component in cyber corporate governance, security, and resilience.

Our research was somewhat limited as a single qualitative empirical study with exclusive focus on the finance sector, specific timing that bridged pre-and post-pandemic conditions, and a narrow set of theoretical lenses. Nevertheless, the strong arguments we present in this paper support our fundamental thesis that strong healthy cyber resilience requires a cyber corporate governance ecosystem.

CHAPTER 7: Conclusion and recommendations

7.1 Introduction

As stated in the Chapter 1 Introduction and each of the three papers (Chapter 4, 5. and 6), this study aimed to investigate the complex issue of leadership and the multi-disciplinary nature of cyber security to help address the significant shortage in existing Leadership in cyber security literature and praxis. These key objectives were based on the central premises for this thesis, which helped guide the development of the questions that needed to be addressed and verified as legitimate claims.

It should be noted that all original premises, questions, and research objectives were my own. Likewise, all the interviews, analysis, models and synthesis were also my own original work. The three articles reporting Phases 1, 2 and 3 were co-authored, so from Chapter 4 onwards, I refer to the researcher/ author in the plural, acknowledging the contribution of my supervisor/co-author, Dr Cate Jerram.

As stated in Chapter 3, this is a qualitative study, so it is necessary to identify the researchers' core assumptions, biases, and premises to the study. The core premises identified and built upon for all three phases of this research are as follows:

Premise #1

Strong cyber security (incorporating cyber hygiene and cyber resilience) is necessary or organisational survival and wellbeing.

Premise #1a

Cyber security is required at every level, and in every department and aspect of the organisation.

Premise #1b

Organisational cyber security must be consistent across the entire organisation. The same policies, rules, and practices must apply in and across all levels, departments, and aspects must be applied.

Premise #2

Cyber risk is an important and often unrecognised element in organisational risk management.

Premise #2a

Cyber risk is multidimensional and multi-disciplined. Cyber defence (hygiene) and resilience therefore need to be multidimensional and multi-disciplined.

Premise #3

Current cyber risk management is dangerously siloed and fragmented.

Premise #4

As an important element of strategic organisational risk management, cyber hygiene and cyber resilience are the responsibility of the organisation's Executive.

Premise #5

Currently, most organisational executives do not recognise or fulfil their role of executive ownership, accountability, and responsibility (OAR) in organisational cyber security.

Premise #6

There is a need to accelerate maturity of the cyber security domain and profession to build a strategic cyber security foundation for effective protection of organisations.

Premise #7

Cyber security has foundations in, and is dependent upon, a variety of disciplinary approaches. These include both the “hard” sciences (e.g., computing and IT) and “soft” disciplines (e.g., psychology and organisational behaviour).

In Phase 1, we introduced the premises formulated by the scoping review. Subsequently, in Phase 2, the principal premises addressed Executives’ failure to understand and strategically value cyber security and executive lack of trust in the CISO, which prevents a unified approach to cyber security and widens the gap in achieving cyber corporate governance ecosystem. Therefore, addressing the following:

Premise #A1

Cyber security needs to be a business issue and fixed into corporate governance.

Premise #A2

Cyber OAR must provide an algorithm for day-to-day managerial decision-making

Premise # A3

Cyber security as a corporate governance must be led by the highest-level executive in the organisation.

Premise # A4

Strategic cyber value must be steered by the expert in cyber security, the CISO.

Premise # A5

CEO-CISO-OAR relationship is absent in organisational cyber corporate governance.

Following Phase 2 analysis, we redefined the question to add a previously unrecognised fundamental premise that true cyber security incorporates cyber resilience (as well as cyber hygiene and protective measures). This premise developed our theory that solid cyber security (resilience) requires a cyber corporate governance ecosystem. To explore and test the validity of this theory and its underlying premise, we identified the following assumptions:

Premise # B1

Cyber security needs to be embedded in corporate governance.

Premise # B2

Cyber security corporate governance must be led by the highest-level executive in the organisation.

Premise # B3

The business ecosystem and the cyber ecosystem need to be incorporated and considered holistically, at both strategic and operational levels.

Premise # B4

The Executive must elevate their CISOs to a strategic role and empowered to fulfil their responsibilities.

Premise # B5

A “cyber security corporate governance ecosystem” as a single conceptual framework has not previously been explored.

7.2 Findings

The major study findings have been described and discussed in the three papers that form the body of this thesis and do not need to be reported here. We will, however, briefly recapitulate our conclusions and recommendations.

7.3 Conclusion and recommendation

A significant conclusion that I can make (with the support of my co-author in three major papers) is that each and every one of the premises that started the study and developed throughout the study have now through a series of scoping and focus literature review and empirical research been verified as legitimate claims. Therefore, they are no longer merely assumptions and premises. This claim in itself is a major contribution.

Conclusions and recommendations from Phase 1 were

1. Traditional silos must be discarded or bridged to enable a strong and holistic multidiscipline of cyber security (**Premises 1, 2 and 3 inclusive**).
2. A new common lexicon must be developed and accepted to enable intelligent and intelligible communication between the different branches of

cyber security and between business and cyber personnel (**Premise 6 and 7**).

3. Most importantly, lexicons and approaches to strategic planning and cyber security need to be aligned in discussion, in practice, and in the Board room (**Premise 4, 5, 6 and 7**).
4. Organisational executives must acknowledge the importance of cyber security and immediately address the role, status, and budget of the CISO (**Premise 1, 2, 4 and 5 inclusive**).
5. Executives must finally take ownership, accountability, and responsibility for their organisation's cyber security (**Premise 4, and 5**).

Building on the recommendations from Phase 1, Phase 2 produced the following conclusions and recommendations:

1. Key mechanisms of corporate governance must promote a shared stewardship approach to balance the probability of cyber risk between key stakeholders (**Premise A1, A2 and A4**).
2. The CEO and the CISO must work together to effectively resolve organisational cyber-OAR issues (**Premise A3, A4 and A5**).
3. The current organisational corporate governance system and mechanisms must change simultaneously and align with the CEO-CISO-OAR relationship (**Premise A1 and A5**).
4. To achieve the aspirational future state of organisational cyber security that we have proposed, organisational cyber security must be embedded in a cyber corporate governance ecosystem (**Premise A1 to A5**).

Phase 3 concluded our study with the following conclusions and recommendations:

1. Triple-loop learning approaches are required to develop from a reactive or superficial reframing and therefore ineffective approaches to cyber security (**Premises, B2, B3 and B5**).
2. Organisations must move from a high-risk fragmented organisational approach to a clear and coherent approach directed by strategic leadership (**Premises B1, B2, B4 and B5**).
3. The business ecosystem and the cyber ecosystem need to be incorporated and considered holistically, at both strategic and operational levels (**Premises B5 and B3**).
4. Cyber security corporate governance must also be led by the highest-level executive in the organisation (**Premise B2, B4 and B5**).
5. It is imperative that the CISO be a strategic trusted advisor in cyber corporate governance, security, and resilience (**Premise B4**).

7.4 Significance of the study

7.4.1 Contributions to practice and theory

A research contribution facilitates in advancing our understanding of the practice or improves the studied practice itself (Ågerfalk & Karlsson 2020). “Adopting a practice-based view thus opens a Pandora’s Box that holds a potential treasure trove for scholars” (Nicolini 2012, p. 77).

As stated in the ‘Conclusions and Recommendation’ section, all the underlying premises we made throughout this study have been explored beyond a literature review, using solid empirical evidence further synthesised with established theory, to verify each premise and legitimatise them as claims. This claim in itself is a significant contribution.

Each of the recommendations listed in ‘Conclusions and Recommendation’ provides and strengthens an understanding of the existing and newly emerging organisational cyber security phenomena and contributes to both theory and practice. The study makes a strong contribution to knowledge for both academia and organisational praxis through a practice- and theory-based ontology defined through a series of models. These models depict the current and an aspirational future state of organisational cyber security.

The study makes two major contributions to practice and theory:

1. Organisational safety and wellbeing requires Cyber security corporate governance that is led by the highest-level executive of the organisation.
2. It is imperative that the CISO be a strategic trusted advisor in cyber corporate governance, security, and resilience.

These two major contributions are umbrella statements that incorporate many component contributions. Each component contribution is distinct and unique but also significantly contributes to the two major contributions. The following paragraphs summarise these important elements.

This study contributes a deeper understanding of the key stakeholders and stakeholder groups in the current fragmented and traditionally siloed cyber environments. Furthermore, it provides a clearer understanding of each stakeholder's role and their loosely interconnected relationships. It clarifies the urgent need to foster cooperation, and build trust to support a united, holistic and strategic approach to organisations' cyber security practice.

An important contribution is our argument for a 'new' unified common lexicon between business and cyber. The future state cyber practice depends upon a common understanding that promotes mutual knowledge-sharing to fill the information gaps and permit intelligent and intelligible communication between business and cyber security. This can only be reasonably achieved with a unified, agreed-upon and new common lexicon.

A consequent contribution of a 'new' common lexicon is that it permits a shared knowledge-base to form. A shared knowledge-based built on a common lexicon would enable a collective approach to enhance and help shape new cyber initiatives that align with strategic plans. This alignment would facilitate intelligent decisions both in practice and the Board room.

The following contribution is twofold. First, the study gives insight into Executive refusal to acknowledge the importance of cyber security, and second brings into focus the diminishing role, status, and budget of the CISO. This study highlights the importance of executives recognising and formalising cyber security's strategic value. And consequently, to immediately shape and address the future

of their Executive CISO to successfully maintain and support a business-cyber led practice.

This research makes a unique contribution to the field of cyber security in proposing that Executives who remain sceptical of cyber security must now step up and take ownership, accountability, and responsibility for their organisation's cyber security to raise awareness, drive change, and achieve a secure organisation ecosystem and resilience.

A significant contribution is that key corporate governance mechanisms must promote a shared stewardship approach to cyber risk shared between the key stakeholders. This shift begins with understanding each key stakeholders' unique role (often tailored by different interests and perspectives) geared towards fostering attitudes and behaviour that support, commit, and form a shared interest in safeguarding a healthy ecosystem.

My model 'Cyber corporate governance ecosystem' (Chapter 6 Figure 6.2) highlights that core business, and the inner circle, have to change. The current profile of cyber-OAR, based on a lack of proper valuation of the strategic nature and importance of organisational cyber security, is not feasible. Our suggestion that the desired state is a partnership where the CEO and the CISO work together as genuine cyber leaders to mitigate risk and execute successful organisational cyber security constitutes a significant contribution, which if followed could radically improve praxis.

A complementary and unique contribution to the not-yet-realised goal of CEO-CISO joint efforts towards organisational cyber security, is identifying of the “corporate governance paradox” and the corporate mechanisms (structure, culture, communication, and trust). Again, if this contribution is accepted, practice must change and align the CEO-CISO-OAR relationship to enable a healthy, cyber secure and resilient organisation.

Organisational cyber security embedded in a cyber corporate governance ecosystem is a valuable contribution of this work. Cyber security must be embedded in core strategy and governance and recognised as critical to the operative environment. Such a shift could enable executives’ visualisation of the big picture. Enabling this insight to identify what is and is not working, would inform better decisions to drive a holistic and converged cyber security strategy.

Another contribution of this research is the recommendation that organisations must revaluate and reflect the current high-risk, fragmented approach to reinvent strategic vision toward a clear, coherent strategic leadership direction. In particular, that the Executive work toward eliminating or bridging internal silos.

An intrinsic contribution is that organisations need to rethink their traditional corporate ownership structures and borders at a strategic and operational level as a cyber ecosystem needs to be incorporated and considered holistically to maintain and promote the ecosystem’s overall health.

The most significant theoretical contribution extends to the application of triple-loop learning (built on the double-loop learning work of Argyris & Schon (1997) in

organisation learning. The use of triple-loop learning in this study is evidence that this theory provides an excellent means by which organisations and leaders can reinvent cyber practice, transform the governing value, and put into practice the cyber corporate governance ecosystem to realise healthy cyber practice and, in turn, achieve resilience.

7.4.2 Further contributions to research

As well as the contributions listed in Contributions to practice and theory section 7.4.1, this research also makes contribution to academia in terms of theory development, future teaching, and further research.

“All models are wrong, but some are useful” is a famous quote often attributed to the British statistician George E. P. Box (Barroso 2018, p. 1). This research contributes a number of useful models. These models can be challenged, taught, and built upon for future research. Figure 4.4 in Phase 1 builds on Porter’s (1980) value chain model. All other figures are original work arising from and illustrating the premises, findings, conclusions, and recommendations of this study of organisational cyber leadership and corporate governance. Some of the earlier models are useful only in terms of sharing the early unedited thinking and workings behind the research (possibly still useful for illustrating research and concept development). Many of the models, however, are valuable illustrations and contributions.

7.5 Limitations of the study and recommendations for future research

As with any research, there are limitations to this study. The major limitations are date and timing, scope and focus, method and methodology. Most of these limitations can be addressed through future research.

7.5.1 Date and timing

Scoping review

Phase 1 of the research, as reported in Chapter 4, Paper 1, has the inherent limitations of an exploratory scoping review. The research in this field is still in its infancy, highlighting extant problems and key gaps, including the absence of substantial research and a heavy reliance on grey literature in this important and rapid evolutionary field. This gap calls for further studies to address the multi-disciplinary domain of cyber security and its leadership.

The focussed depth literature review

Our research was built on the scoping review and undertook a focussed literature review to help hone in on subject-relevant sources. Gaps that needed further investigation rapidly became apparent alongside the evident absence of substantial research. This absence highlights the need for further research beyond the work presented in this thesis.

Removing biases can be challenging and subtle nuances in the data might be missed (Tisdale 2016, p. 71). Therefore, during each phase of our research, we

constantly revisited the predefined premises to identify any unrecognised bias and confirm the identified biases and underlying approach. We recommend future research using our results and findings to challenge and/or confirm our interpretation.

Empirical study

In the empirical phase of our study, Phase 2 (as reported in Paper 2, Chapter 5) commenced during the initial and early impact of the COVID-19 pandemic. This timing was both a strength and a limitation of our research. The empirical data was collected pre-and during the first wave and peak of the pandemic.

Too early for academic publications, some interesting trends and insights were presented through grey literature on the emerging role of CISO as organisations were confronted with additional cyber challenges, including the need for unprepared remote work circumstances, and exponentially increasing cyber-attacks. Exploring the “new normal” CISO role and the changes in organisational cyber security throughout the roller coaster ups and downs of COVID-19 pandemic, plateau and successive waves, provides a platform and can act as a catalyst for future research.

Theory

Stakeholder theory was used throughout, shaping the research proposal and each phase of the study. Possibly, future research into the cyber corporate governance ecosystem that is based on a different theory might steer the findings in a different direction.

Triple-loop learning theory has a very specific perspective that was brought to this research. If future research analysed our data and findings through a different theoretical lens, other and different conclusions and recommendations could well result.

7.5.2 Scope and focus

Scoping review broad

As the research objective ‘leadership in cyber security’ is inherently complex with considerable scope and scale, we set tight-binding parameters to maintain control. We decided to focus only on one industry being the finance and accounting industry-sector and limited our investigation to large global enterprises. This predefined scope granted us access to truly rich insights about strategic leadership, CISOs, cyber security, strategy and corporate governance. The valuable lesson learnt in these specific areas from our research could be widely applied across general and multiple sector-specific industries. However, this transferability and breadth of applicability require further research with more specific definition and until such research is conducted, this is a limitation of our findings.

We propose a future that can address the same research problem and leverage from our findings across different industry-sectors and business size classifications as well as the different disciplines (such as Marketing and Human Relations (HR) within business. We do touch on HR in our research, and from the

findings affirm that HR is an area that demands its own in-depth research, specifically on the role of Executive HR in cyber culture and cyber awareness.

7.5.3 Method and methodology

Method

Applying a qualitative approach to our research objective granted the flexibility to explore new and related prior work, providing a deeper understanding of current issues facing leadership in cyber security.

Each phase of the research was exploratory and qualitative. While providing depth, this approach provided limited coverage. For instance, the absence of quantitative measures at the early stage meant that small numbers do not permit generalisability. Biases were acknowledged with no claim to objectivity; premises were stated and challenged but no hypotheses were made or tested.

A quantitative approach cannot be instituted on our full research objective until further qualitative research is carried out on key areas and subtopics indicated in our research. Nevertheless, it is possible for researchers to consider a quantitative study to challenge and/or verify our results by gathering critical data for richer testing (or a hybrid approach mixed design studies to repeat, expand, and test our research). However, we strongly recommend that more focussed qualitative exploration is necessary before the field is ready for quantitative verification study.

Theory

Although the theoretical lenses employed have provided rich insight, there are other theories we have not explored. Stakeholder theory proved a powerful lens across all three phases of our research, but future research could work from a different foundation.

Although we also drew lightly on institutional and upper echelon theories, we only touched the edges of these theories. Each or either of these lenses could be an effective filter to investigate this work. We suggest that these theories and others that we have not touched on would be suitable for future research, adding a different lens and valuable insight to investigate these issues.

The broader and more complex theory of triple loop learning theory was selected for depth and relevance given our specific scope and focus. An un-investigated possibility is the application of a double-loop lens to provide a related but different in-depth study. In fact, there are many appropriate theories that could brought to this research to provide different insights or confirm our conclusions and recommendations.

The models illustrating our findings and concepts, although contributions of value as theory generated from, through and by this research, are still inherently limited and flawed (‘All models are wrong, but some are useful’).

As ever, in qualitative work, removing our conscious and unconscious biases during the process has been challenging. To mitigate any implicit personal bias impacting our research, we routinely returned to our premises to challenge our,

our conscious and unconscious biases, assumptions, and beliefs, but we could have missed something. Moving forward, we need other researchers who are not invested in our theory or tied to our beliefs, assumption, and premises to use, test and challenge our theory (with or without our data) to give our theory strength and value and to confirm its usefulness and transferability.

7.5.4 Future research – further details

We conclude by detailing the already suggested concepts and other suggestions of highly needed future research listed below. Further research is needed on our model of ‘cyber corporate governance ecosystem’ to refine, challenge and expand our work. It would also be valuable to build upon the triple-loop learning lens with other theories. Moreover, further work is needed to design and model-specific architecture (at both strategic and operational levels) in cyber organisational practice. following our recommendations.

Building upon our research findings, we propose avenues for future research, particularly in sectors we have not visited, such as manufacturing, petroleum, or medicine. The themes that warrant further investigation include the CEO-CISO-OAR, their relationship, the strategic value executive placed on cyber security, and the immediate need for the executive to address the role, status, and budget of the CISO.

The siloed, fragmented state of organisational cyber security remains a current challenge demanding immediate attention and is worthy of further research. We

suggest a detailed stakeholder analysis to understand both challenges and victories and to find key commonalities or shared interests and challenges.

A new common lexicon across the identified silos and different industry-sectors would be valuable but was outside our research scope. We suggest identifying the common, standard terms, phrases, and definitions to investigate how these terms are used and understood throughout the cyber corporate governance ecosystem, including boardroom discussions. After analysing these insights, work could begin on forming a new lexicon.

Further studies are needed to investigate HR and their corporate role as ‘keepers of the organisational culture’, which was only touched upon in our study. It is an important area often neglected in cyber research.

7.6 Implications for stakeholders in cyber security

An implication exists in relation to a contribution – that is, a research contribution leads to implications with regard to particular practices (Ågerfalk & Karlsson 2020, p. 109). Based on the findings in our research the following implications are needed to unite to develop a strong multi-disciplinary cyber community and ecosystem. Traditional silos must be discarded to enable a strong and holistic multidiscipline of cyber security.

Government and quasi-governmental

Government and quasi-governmental regulators play a lead and vital role in cyber security in that they:

- should continue to lead, guide and drive cyber initiatives to raise awareness and work to benchmark regulations, standards and practice.
- must adapt to a more collaborative, co-design, and co-production approach with the cyber sector and industry for successful acceptance.
- should act in furtherance of the cyber leadership issue, and work to and entrench executive responsibility for organisational cyber security in law.

Vendors, outsourced providers, and consultants

Vendors, outsourced providers, and consultants must play a key advisory role.

These stakeholders have the added advantage as part of their normal business activity of communicating and working across-disciplines and across-industries inter-operably, which could help guarantee a mutually agreed-upon orchestrated response to cyber threats.

This requires putting aside their differences and moving towards a new coherent mix of competition and cooperation known as co-opetition.

Disciplines, professional bodies, and cyber educators

Disciplines, professional bodies, and cyber educators should acknowledge the dangers of traditional interdisciplinary and silo attitudes.

Only then can they de-emphasise their differences, strengthen the collaboration and establish synergies, all critical elements in advancing cyber security as a multi-disciplinary field in its own right.

CISO

The CISO must emerge as a trusted and vital strategic advisor. Their responsibility for information and cyber security programs should extend across the entire ecosystem. CISO also need to assume responsibilities outside their siloed and specialised domain knowledge and be able to communicate and collaborate cross-functionally and cross-domains. CISOs require business acumen skills (management and communication). And a combination of IT-oriented-security and business-oriented-security is essential to help organisations' leaders make better cyber decisions.

Executives

Executives need to move from standard textbook management practices -where cyber security does not appear - to real digital world practice.

Cyber security must no longer sit outside the Executive's remit, but underlying assumptions must be examined, and all aspects of cyber security be embedded in corporate governance and mechanisms.

Cyber security needs to be embedded in culture and set from the top to raise awareness and send a consistent message.

Executives need to garner assistance from the multistakeholder cyber community, especially from the CISO. They must also recognise, formalise the strategic value of cyber security, and promote the CISO to a strategic trust advisor and partner.

Executives need to lead and take an integral, holistic approach by coordinating, determining priorities, and breaking down barriers to meet this challenge.

REFERENCES

Abawajy, J 2014, “User preference of cyber security awareness delivery methods”, Behaviour & Information Technology, vol. 33, no. 3, pp. 237–248, DOI 10.1080/0144929x.2012.708787, <http://dx.doi.org/10.1080/0144929X.2012.708787>.

Absolute 2019, “What is Regulatory Compliance”, Absolute Team, Absolute, May, Accessed 15/10/2020, <https://www.absolute.com/blog/what-is-regulatory-compliance/>.

ACS 2016, “Cybersecurity – Threats Challenges Opportunities”, Australia Computer Association (ACS), Nov, pp. 1–72, viewed 20/06/2018, <https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf>.

ACSC 2020, “ACSC Annual Cyber Threat Report July 2019 to June 2020 Australian Cyber Security Centre”, *Australian Cyber Security Centre (ACSC), Australian Government*, Jun, p. 18, <https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2019-june-2020>.

ACSC 2020, ASD Cyber Skills Framework, Australian Cyber Security Centre (ASCS), Australian Government, viewed 29/11/2020, <https://www.cyber.gov.au/acsc/view-all-content/publications/asd-cyber-skills-framework>.

ACSC 2021, “ACSC Annual Cyber Threat Report 1 July 2020 to 30 June 2021', Australian Cyber Security Centre (ACSC), Australian Government, pp. 1–56, viewed 11/10/2021, <https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21>.

Adhikarl, S 2019, “Banks, insurers and superannuation funds making basic cyber security errors, says APRA”, The Australian, Nov, pp. 1–3, viewed 23/01/2021, <https://www.theaustralian.com.au/business/technology/banks-insurers-and-superannuation-funds-making-basic-cyber-security-errors-says-apra/news-…>.

Adnan, A & Ahmed, N 2019, “The transformation of the Corporate Governance Model: A literature review”, Copernican journal of finance & accounting, vol. 8,

no. 3, 7, pp. 7–47, DOI 10.12775/CJFA.2019.011, <http://dx.doi.org/10.12775/CJFA.2019.011>.

Adnan, H 2016, The difference between Cybersecurity and Information Security, PECB, Social Media Manager viewed 19/8/2019, <https://www.slideshare.net/PECBCERTIFICATION/the-difference-betweencybersecurity-and-information-security>.

Ågerfalk, PJ & Karlsson, F 2020, “Artefactual and empirical contributions in information systems research”, European Journal of Information Systems, vol. 29, no. 2, pp. 109–113.

Althonayan, A & Andronache, A 2019, “Resiliency under Strategic Foresight: The effects of Cybersecurity Management and Enterprise Risk Management Alignment”, paper presented at Conference: Published in: 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Oxford, MS, USA, June 3–4;pp.1-9.

Antonucci, D 2017, The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities, John Wiley & Sons, Hoboken, New Jersey, US, viewed 27/10/2018, DOI 10987654321.

APRA 2020, “Executive Board Member Geoff Summerhayes – speech to Financial Services Assurance Forum”, APRA, Nov, pp. 1–8, viewed 12/01/2020, <https://www.apra.gov.au/news-and-publications/executive-board-member-geoff-summerhayes-speech-to-financial-services>.

Argyris, C 1976, “Single-Loop and Double-Loop Models in Research on Decision Making”, Administrative Science Quarterly, vol. 21, no. 3, pp. 363–375, <http://www.jstor.org/stable/2391848>.

Argyris, C 1977, “Double loop learning in organizations”, Sept-Oct, Harvard Business Review, vol. 55, no. 5, Sept-Oct, pp. 115-125.

Argyris, C 1998, “Empowerment: the emperor's new clothes”, Harvard Business Review, vol. 76, no. 3, May-Jun, pp. 98–105, <https://www.ncbi.nlm.nih.gov/pubmed/10179657>.

Argyris, C 2003, “Argyris: A Life Full of Learning”, Organization Studies, vol. 24, no. 7, pp. 1178–1192. <https://doi.org/10.1177/01708406030247009>.

Argyris, C & Schon DA 1997, “Organizational Learning: A Theory of Action Perspective”, Revista Española de Investigaciones Sociológicas, pp. 345–348.

Ashkenas, R 2015, “Jack Welch’s Approach to Breaking Down Silos Still Works”, Harvard Business Review, pp. 2–4. <https://hbr.org/2015/09/jack-welchs-approach-to-breaking-down-silos-still-works>.

Aston, T 2020, “Assumptions and triple loop learning”, Medium, Dec, pp. 1–6, viewed 25/10/2021, <https://thomasmtaston.medium.com/assumptions-and-triple-loop-learning-c9699dacbeab>.

AustCyber 2019, “Australia’s Cyber Security Sector Competitiveness Plan 2019 Update”, Australian Government, Industry Gowth Centres, Dec, pp. 1–156, viewed 8/07/2020, <https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2019>.

AustCyber 2021, “Recommendations Report – NSW Cyber Security Standards Harmonisation Taskforce”, AustCyber|Standards Australia, Jan, pp. 1–16, viewed 30/01/2021, <https://www.austcyber.com/news-events/cyber-security-taskforce-releases-priority-recommendations>.

Australian Government 2019, “Proposal Paper 22 January 2020 -Implementing Royal Commission Recommendations 3.9, 4.12, 6.6, 6.7 and 6.8 Financial Accountability Regime', The Treasury, Commonwealth of Australia, pp. 1–18, viewed 12/01/2021, <https://treasury.gov.au/sites/default/files/2020-01/c2020-24974.pdf>.

Australian Government 2020, “Australia’s Cyber Security Strategy 2020”, Cyber, Digital and Technology Policy Division, Commonwealth of Australia, Aug, pp. 1–52, viewed 10/10/2020, <https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf>.

Bakari, JK., Tarimo, CN., Yngström, L., Magnusson, C and Kowalski, S 2007, “Bridging the gap between general management and technicians – A case study on ICT security in a developing country”, Computers & Security, vol. 26, no. 1, pp. 44–55, DOI 10.1016/j.cose.2006.10.007.

Barroso, G 2018, “All models are wrong, but some are useful”. George E. P. Box, AdMoRe ITN, <https://www.lacan.upc.edu/admoreWeb/2018/05/all-models-are-wrong-but-some-are-useful-george-e-p-box/>.

Bayuk, J 2009, “How to write an information security policy”, CSO, Jun, pp. 1–7, viewed 18/03/2019, <https://www.csoonline.com/article/2124114/strategic-planning-erm-how-to-write-an-information-security-policy.htm>.

Benjamin, R 2014, “Tone at the Top – Today’s Biggest Cyber-Security Weakness”, eForensics Magazine, Sep, pp. 1–4, viewed 19/01/2021, <https://eforensicsmag.com/tone-at-the-top-todays-biggest-cyber-security-weakness-by-rob-benjamin/>.

Bhatt, GD 2000a, “An empirical examination of the effects of information systems integration on business process improvement”, International Journal of Operations & Production Management, vol. 20, no. 11, pp. 1331–1359.

Bhatt, GD 2000b, “A resource-based perspective of developing organizational capabilities for business transformation”, Knowledge and Process Management, vol. 7, no. 2, pp. 119–129.

Björck, F., Henkel, M., Stirna, J and Zdravkovic, J 2015, “Cyber Resilience – Fundamentals for a Definition”, Advances in Intelligent Systems and Computing”·, Jan, p. 7, DOI 10.1007/978-3-319-16486-1_31.

Bjorn-Andersen, N & Raymond, B 2014, “The impact of IT over five decades – towards the Ambient organization”, Applied Ergonomic, vol. 45, no. 2, pp. 188–197, DOI 10.1016/j.apergo.2013.04.025, <https://www.ncbi.nlm.nih.gov/pubmed/23820665>.

Bloomenthal, A 2021, “C-Suite Definition”, Investopedia, Feb, pp. 1–6, viewed 03/05/2021, <https://www.investopedia.com/terms/c/c-suite.asp>.

Bond, R 2017, “Why Organizations Aren’t Using Cybersecurity Frameworks”, HITACHI, December 14, Accessed: 4/12/2019, <https://www.hitachi-systems-security.com/blog/cybersecurity-frameworks-challenges/>.

Boulton, C 2018, “CIO playbook: 10 tips for leading IT in the digital era”, CIO, Jun, pp. 1–6, viewed 5/07/2019, <https://www.cio.com/article/3279884/cio-playbook-10-tips-for-leading-it-in-the-digital-era.html>.

Breitrose, P n.d., “Chapter 30. Section 1. Overview: Getting an Advocacy Campaign Off the Ground”, Community Tool Box, pp. 1–8, viewed 10/02/2021, <https://ctb.ku.edu/en/table-of-contents/advocacy/advocacy-principles/overview/main>.

Bundy, J., Vogel, RM and Zachary, MA 2017, “Organization–stakeholder fit: A dynamic theory of cooperation, compromise, and conflict between an organization and its stakeholders”, Strategic Management Journal, vol. 39, no. 2, pp. 476–501, DOI 10.1002/smj.2736.

Burns, AJ., Posey, C., Roberts, TL and Benjamin Lowry, P 2017, “Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals”, Computers in Human Behavior, vol. 68, pp. 190–209.

Buxton, N 2019, “Multistakeholderism: a critical look – Workshop Report, Amsterdam”, Transnational Institute (TNI), Mar, pp. 1–16, viewed 1/06/2020, <https://www.tni.org/files/publication-downloads/multistakeholderism-workshop-report-tni.pdf>.

Caisley, O 2021, “Australian companies ignoring risk of cyber attacks”, The Australian, Oct, pp. 1–2, viewed 4/11/2021, <https://www.theaustralian.com.au/business/technology/australian-companies-ignoring-risk-of-cyber-attacks/news-story/dae5b1189d1da89eacfd10…>.

Caravella, KD 2011, “Mimetic, coercive, and normative influences in institutionalization of organizational practices: The case of distance learning in higher education”, Faculty of The College for Design and Social Inquiry, Florida Atlantic University.

Carlson, B 2021, “Top cybersecurity statistics, trends, and facts”, CSO Online, Oct, pp. 1–8, viewed 12/10/2021, <https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html>.

CGI 2019, “Cyber Security in the Boardroom: UK plc at risk”, Apr, pp. 1–28, viewed 20/11/2020, <https://www.cgi.com/sites/default/files/2019-04/cyber-security-launch-white-paper.pdf>.

Chachak, E & Fischoff, Y 2019, “Cybersecurity Industry Report:Are You Ready for the MSSP Revolution?”, CyberDB, Oct, pp. 1-28, viewed 24/10/2019, <https://www.cyberdb.co/wp-content/uploads/2019/10/CyberDB-Industry-Report-MSSP-market-V2.pdf>.

Chamberlain, C 1991, “Charleston Conference 1990 – The Gatekeeper and Information”, Library Acquisitions: Practice & Theory, vol. 1, no. 15, pp. 265–269.

Chen, WH., Kang, MP and Butler, B 2019, “How does top management team composition matter for continual growth? Reinvestigating Penrose’s growth theory through the lens of upper echelons theory”, Management Decision, vol. 57, no. 1, pp. 41–70, DOI 10.1108/md-02-2017-0147.

Chertoff 2018, “How to Increase Cybersecurity Competence in Boards and Management”, The Chertoff Group, ABA Law Practice Today., Feb, pp. 1–3, viewed 22/09/2021, <https://www.lawpracticetoday.org/article/cybersecurity-competence-boards-management/>.

Choo, K-KR., Smith, RG and McCusker, R 2007, “Future directions in technology-enabled crime: 2007–09”. Research and Public Policy Series no. 78. Canberra, Australian Institute of Criminology, Australian Government, pp. 1–166, viewed 29/03/2019, < https://aic.gov.au/publications/rpp/rpp78>.

Christensen, KK & Petersen, KL 2017, “Public–private partnerships on cyber security: a practice of loyalty”, Journal of International Affairs, vol. 93, no. 6, Nov, pp. 1435–1452, DOI 10.1093/ia/iix189.

Clark, DD & Wilson, DR 1987, “A Comparison of Commercial and Military Computer Security Policies”, 1987 IEEE Symposium on Security and Privacy, Apr, pp. 184–184, DOI 10.1109/sp.1987.10001, <https://ieeexplore.ieee.org/document/6234890/>.

Colwill, C 2009, “Human factors in information security: The insider threat – Who can you trust these days?”, Information Security Technical Report, vol. 14, no. 4, pp. 186–196, DOI 10.1016/j.istr.2010.04.004.

Craigen, D., Diakun-Thibault, N and Purse, R 2014, “Defining Cybersecurity”, Technology Innovation Management Review, pp. 13–21.

Crozier, R 2019, “Aussie IT Firms cop customer trust hits as encryption laes bite”, ITNews, Feb, pp. 1–7, viewed 30/03/2019, <https://www.itnews.com.au/news/aussie-it-firms-cop-customer-trust-hit-as-encryption-laws-bite-519286>.

CSOMag 2018, “There is no better time than now to get into cybersecurity”, CSOMag, Nov, pp. 1–3, viewed 1/04/2021, <https://cisomag.eccouncil.org/there-is-no-better-time-than-now-to-get-into-cybersecurity/>.

Da Veiga, A & Eloff, JHP 2007, “An Information Security Governance Framework”, Information Systems Management, vol. 24, no. 4, pp. 361–372, DOI 10.1080/10580530701586136, <https://doi.org/10.1080/10580530701586136>.

Daud, M., Rasiah, R., George, M., Asirvatham, D and Thangiah, G 2018, “Bridging the Gap Between Organisational Practices and Cyber Security Compliance: Can Cooperation Promote Compliance in Organisations”, International Journal of Business and Society, vol. 19, no. 1, pp. 161-180.

Davis, RE 2017, “Relationship between Corporate Governance and Information Security Governance Effectiveness in United States Corporations”, College of Management and Technology, Dissertations and Doctoral Studies thesis, Walden University.

Davidoff, S 2019, *Data breaches: Crisis and Opportunity*, Addison-Wesley Professional.

Debernardi, W 2021, “Knowledge is power – but where is your data”, Public Accountants, Apr, pp. 1–3, viewed 20/10/2021, <https://www.publicaccountant.com.au/blog/knowledge-is-power-but-where-is-your-data>.

Deloitte 2019, “Is Cyber on the Board’s Agenda?”, Wall Street Journal Risk & Compliance Journal, Jun, pp. 1–4, viewed 12/8/2020, <https://deloitte.wsj.com/riskandcompliance/2019/06/04/is-cyber-on-the-boards-agenda/>.

Deloitte 2020, “Financial Accountability Regime (FAR) At a glance September 2020”, Sep, pp. 1–13, viewed 12/01/2021, <https://www2.deloitte.com/content/dam/Deloitte/au/Documents/audit/deloitte-au-far-glance-september-2020-101020.pdf>.

Dunning, D 2011, “The Dunning–Kruger Effect”, in Advances in Experimental Social Psychology, vol. 44, Elsevier Inc., Ithaca, New York, USA, pp. 247-296.

Edgar, T & Manz, D 2018, “Research Methods for Cyber Security”, Network Security, vol. 1, no. 6, p. 5, viewed 01/09/2019, <http://bit.ly/2JCIPQE.>.

Elkhannoubi, H & Belaissaoui, M 2015, “A framework for an effective cybersecurity strategy implementation: Fundamental pillars identification”, paper

presented at 2015 15th International Conference on Intelligent Systems Design and Applications (ISDA), Marrakech, DOI:10.1109/ISDA.2015.7489156.

Ellis, S 2016, “Chief Information Handbook Security Officer”, CISO Handbook Federal Working Group, CISO Council, CIO Council, Incapsulate, LLC and REI Systems, Inc., pp. 1–170, viewed 19/01/2019, <https://www.cio.gov/assets/files/CISO_Handbook.pdf>.

Enns, HG., Huff, SL and Higgins, CA 2003, “CIO Lateral Influence Behaviors – Gaining Peers' Commitment To Strategic Information Systems”, MIS Ouarterly, vol. 27, no. 1, Mar, pp. 155–176, DOI 10.2307/30036522, <https://www.jstor.org/stable/30036522>.

Farnam Street 2013, “The Two Types of Ignorance”, FS Nov, viewed:23/09/2021, <https://fs.blog/2013/11/two-types-of-ignorance/>.

Fenwick, M, & McCahery, JA, and Vermeulen, EPM 2019, “The End of ‘Corporate’ Governance: Hello ‘Platform’ Governance”, European Business Organization Law Review, vol. 20, no. 1, Feb, pp. 171-199, DOI 10.1007/s40804-019-00137-z, <https://doi.org/10.1007/s40804-019-00137-z>.

Fitzgerald, T 2018, CISO COMPASS: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers, CRC Press.

FPA 2018, “A landmark code monitoring cooperation agreement announced by professional associations”, Dec, pp. 1–4, viewed 2/2/2021, <https://fpa.com.au/news/a-landmark-code-monitoring-cooperation-agreement-announced-by-professional-associations/>.

Frauenstein, EE & Von Solms, R 2014, “Combatting phishing: A holistic human approach”, Information Security for South Africa, pp. 1–10.

Freeman, RE., Phillips, R and Sisodia, R 2018, “Tensions in Stakeholder Theory”, Business & Society, vol. 59, no. 2, pp. 213–231, DOI 10.1177/0007650318773750.

Freeman, RE., Wicks, AC and Parmar, B 2004, “Stakeholder Theory and "The Corporate Objective Revisited”, Organization Science, vol. 15, no. 2, pp. 364–369, DOI 10.1287/orsc.1040.0066.

Fruhlinger, J 2019, “What is a CISO? Responsibilities and requirements for this vital leadership role”, CSO, Jan, pp. 1–8, viewed 10/11/2019, <https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html>.

GAP 2017, “Protecting The New Frontier Report, Gap Taskforce On Cyber Security”, Global Access Partners (GAP), Nov, pp. 1–50, viewed 15/09/2020, <http://www.globalaccesspartners.org/Cyber_Security_Taskforce_Report_GAP_Nov2017.pdf>.

Gartner 2021, “Gartner Survey Finds 88% of Boards of Directors View Cybersecurity as a Business Risk”, Nov, pp. 1–3, viewed 20/12/2021, <https://www.gartner.com/en/newsroom/press-releases/2021-11-18-gartner-survey-finds-88-percent-of-boards-of-directors-view-cybersecurity-as-a…>.

Gleeson, B 2013, “The Silo Mentality: How To Break Down The Barriers”, Forbes, Oct, pp. 1–5, viewed 1/05/2021, < https://www.forbes.com/sites/brentgleeson/2013/10/02/the-silo-mentality-how-to-break-down-the-barriers/ >.

Goodyear, M., Goerdel, HT., Portillo, S and Williams, L 2010, “Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers, Strengthening Cybersecurity Series”, IBM Center for The Business of Government, pp. 1–42, viewed 17/07/2018, <https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/cybersecurity-management-in-the-states-ibm-kansas-u-report-may-2010.pdf>.

Goyder, M 2002, “Lessons from Enron”, Tomorrow’s Company, Jul, pp. 1–11, viewed 20/12/2019, <https://www.tomorrowscompany.com/publication/799/>.

Greef, L de., Post, G., Vink, C and Wenting, L 2017, Chapter 1 Introduction, Designing Interdisciplinary Education : A Practical Handbook for University Teachers –, Amsterdam University Press, <https://www.jstor.org/stable/j.ctt1sq5t4k>.

Green, H 2016, “IT Makes Good Career Sense To Belong To An Association Or Body Linked To Your Profession Or Trade”, Career Confident, Sep, pp. 1–6, viewed 1/05/2019, <https://careerconfident.com.au/makes-good-career-sense-belong-association-body-linked-profession-trade/>.

Greene, SS 2014, “Security Policies and Procedures: Principles and Practices, Second Edition”, Pearson Education, Inc., Jul, pp. 1–638, DOI 10: 0-7897-5167-

4,
<http://ptgmedia.pearsoncmg.com/images/9780789751676/samplepages/0789751674.pdf>.

Gupta, A., Briscoe, F and Hambrick, DC 2018, “Evenhandedness in Resource Allocation: Its Relationship with CEO Ideology, Organizational Discretion, and Firm Performance”, Academy of Management Journal, vol. 61, no. 5, pp. 1848–1868, DOI 10.5465/amj.2016.1155.

Hambrick, DC 2007, “Upper Echelons Theory: An Update”, Academy of Management Review, vol. 32, no. 2, 334–343, DOI 10.5465/AMR.2007.24345254.

Haney, JM & Lutters, WG 2017, “The Work of Cybersecurity Advocates”, in Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems - CHI 2017, May 6–11, 2017, Denver, CO, USA, pp. 1663–1670.

Haney, JM & Lutters, WG 2018, “‘It’s Scary...It’s Confusing...It’s Dull’: How Cybersecurity Advocates Overcome Negative Perceptions of Security”, In Fourteenth Symposium on Usable Privacy and Security (SOUPS'18), August 12–14; Baltimore, MD, USA, pp. 411–425.

Harvey, L 2004, Professional body, Analytic Quality Glossary, Quality Research International, viewed 21/05/2019, <http://www.qualityresearchinternational.com/glossary/>.

Hasib, M 2015, “Cybersecurity Leadership: Powering the Modern Organization”, Third Edition, Tomorrow’s Strategy Today, LLC.

Hendry, J 2019, “Atlassian says encryption-busting laws threaten jobs”, ITNews, Mar, viewed 2/09/2019, <https://www.itnews.com.au/news/atlassian-says-encryption-busting-laws-threaten-jobs-523007>.

Hepfer, M & Powell, TC 2020, “Make Cybersecurity a Strategic”, MIT Sloan Management Review, vol. 62, no. 1, Fall, pp. 40–45.

Hilton, J 2016, “Why HR is critical in cybersecurity”, HRD Australia, Dec, pp. 1–5, viewed 9/05/2019, <https://www.hcamag.com/au/news/general/why-hr-is-critical-in-cybersecurity/147632 >.

Hitchcock, L 2007, “Industry Certification and Academic Degrees: Complementary, or Poles Apart? ”, in 2007 SIGMIS CPR Conference, April 19–21, St Louis MO. Proceedings published in the ACM Digital Library.

Hoffman, LJ., Burley, DL and Toregas, C 2011, “Thinking Across Stovepipes: Using a Holistic Development Strategy to Build the Cybersecurity Workforce”, IEEE Security and Privacy, DOI 10.1109/MSP.2011.181, <https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/stovepipes_gw_cspri_report_2011_8_0.pdf>.

Homeland Security 2020, “News Release: DHS Awards $2M to University of Illinois-led Consortium to Create National Network of Cybersecurity Institutes”, Oct, pp. 1–3, viewed 29//01/2021, <https://www.dhs.gov/science-and-technology/news/2020/10/30/news-release-dhs-awards-2m-create-national-cybersecurity-network>.

Hörisch, JR., Freeman, E and Schaltegger, S 2014, “Applying Stakeholder Theory in Sustainability Management: Links, Similarities, Dissimilarities, and a Conceptual Framework”, Organization & Environment, vol. 27, pp. 328–346.

Houchens, GW & Keedy, JL 2009, “Theories of Practice: Understanding the Practice of Educational Leadership”, Journal of Thought, vol. 44, pp. 49–61.

Hoyle, S 2014, “Industry or professional, if you’re talking about an association the difference matters”, Professional Planner, Jul, pp. 1–3, viewed 1/05/2019, <https://www.professionalplanner.com.au/2014/07/industry-or-professionthe-difference-matters/>.

Hudson, M 2018, “Upper Echelon Theory”, Marc Hudson, Accessed:7/09/2021, <https://marchudson.net/academia/policy-terms-alphabetical-list/upper-echelon-theory/>.

Hunter, AP 2018, “Economic Security as National Security: A Discussion with Dr. Peter Navarro”, in Center for Strategic and International Studies (CSIS), Superior Transcriptions LLC, CSIS Headquarters, Washington, D.C.

ICAEW 2012, “The Role And Structure Of Professional Bodies: Current And Future Challenges – A roundtable discussion prepared by ICAEW and hosted by CECCAR”, paper presented at Central Eastern and South eastern Europe Regional Conference Sinaia, Romania, 26–27 January.

Intellect IT 2020, “Intellect ITs response to Prime Minister’s Announcement of Cyber Attack”, Intellect Information Technology, Jun, pp. 1–2, viewed 18/02/2020, <https://www.intellectit.com.au/news/intellect-its-response-to-prime-ministers-announcement-of-cyber-attack/>.

ISC2 2020, “(ISC)² Partners with AISA to Advance Cybersecurity in Australia”, ISC2, Feb, pp. 1–5, viewed 16/01/2021, <https://www.isc2.org/News-and-Events/Press-Room/Posts/2020/02/05/ISC2-Partners-with-AISA-to-Advance-Cybersecurity-in-Australia>.

ISC2 2020, “Cybersecurity Professionals Stand Up to a Pandemic”, (ISC)2 Cybersecurity Workforce Study– 2020, pp. 1–43, viewed 16/01/2021, <https://www.isc2.org/Research/Workforce-Study>.

ITU-T 2008, “Overview of cybersecurity”, ITU-T X.1205 SERIES X: Data Networks, Open System Communications and Security Telecommunication security, Apr, pp. 1–64, <https://www.itu.int/rec/T-REC-X.1205-200804-I/en>.

Jayne, J 2020, “(Cyber) Security Culture Eats (Cyber) Security Strategy for Breakfast”, Australian Cyber Security Magazine, Sep, pp. 1–5, viewed 19/05/2021, <https://australiancybersecuritymagazine.com.au/cyber-security-culture-eats-cyber-security-strategy-for-breakfast/>.

Joanna Briggs Institute 2020, The Scoping Review Network, 20/02/2020, <https://jbi.global/scoping-review-network/network>.

Johannessen, Å., Gerger Swartling, Å., Wamsler, C., Andersson, K., Arran, JT., Hernández Vivas, DI and Stenström, TA 2018, “Transforming urban water governance through social (triple-loop) learning”, Environmental policy and governance, vol. 29, no. 2, pp. 144–154, DOI 10.1002/eet.1843.

Kappers, WM & Harrell, N 2020, “From Degree to Chief Information Security Officer (CISO): A Framework for Consideration”, Journal of Applied Business and Economics, vol. 22, no. 11, pp. 260–288.

Karanja, E & Rosso, MA 2017, “The Chief Information Security Officer_ An Exploratory Study”, Journal of International Technology and Information Management, vol. 26, no. 2, pp. 23–47.

Karanja, E 2017, “The role of the chief information security officer in the management of IT security”, Information & Computer Security, vol. 25, no. 3, pp.

300–329, DOI 10.1108/ics-02-2016-0013, <www.emeraldinsight.com/2056-4961.htm>.

Kay, R & Goldspink, C 2015, “When does good governance lead to better performance”, Australian Institute of Company Directors, pp. 1–20, <http://www.companydirectors.com.au/~/media/resources/director-resource-centre/glc/kay-governance-report-whitepaper-report.ashx?la=en>.

Kiryakova, G 2019, “Cybersecurity Standoff Australia”, UNISYS, Oct, pp. 1–12, viewed 18/10/2019, <https://assets.unisys.com/Documents/AU/WP_191014_CyberSecurityStandoffAustralia.pdf>.

Knapp, KJ., Maurer, C and Plachkinova, M 2017, “Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance”, Journal of Information Systems Education, vol. 28, no. 2, Dec, pp. 101–114, viewed 14/11/2019, <http://jise.org/Volume28/n2/JISEv28n2p101.html>.

Knight, E 2018, “Are banks irresponsible about responsible lending?”, SMH, Mar, pp. 1–3, viewed 9/07/2021, <https://www.smh.com.au/business/banking-and-finance/are-banks-irresponsible-about-responsible-lending-20180320-p4z5bh.html>.

Kotter, JP 2014, “Capturing the Opportunities and Avoiding the Threats of Rapid Change”, Leader to Leader, pp. 32–37.

Kovsky, S 2019, “Where Do CISOs Belong in an IT Org Chart?”, InformationWeek, May, pp. 1–5, viewed 12/05/2021, < https://www.informationweek.com/cybersecurity/where-do-cisos-belong-in-an-it-org-chart- >.

Kuerbis, B & Badiei, F 2017, “Mapping the cybersecurity institutional landscape”, Digital Policy, Regulation and Governance, vol. 19, no. 6, pp. 466–492, DOI 10.1108/dprg-05-2017-0024.

Labib, AW 2016, “Towards a Triple Loop Learning from Failures”, in 13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13), Sheraton Grande Walkerhill Seoul, Korea, pp. 1–10.

Lankton, N., Price, JB and Karim, M 2021, “Cybersecurity Breaches and the Role of Information Technology Governance in Audit Committee Charters”, Journal of Information Systems, vol. 35, no. 4, pp. 101–119.

Lappi, T 2017, “Formation and governance of a healthy business ecosystem”, Acta Universitatis Ouluensis, C Technica, vol. C 626, pp. 1–114.

Lappi, T., Lee, TR and Aaltonen, K 2017, “Assessing the Health of a Business Ecosystem: The Contribution of the Anchoring Actor in the Formation Phase”, International journal of management, knowledge and learning, vol. 6, no. 1, pp. 27–51.

Lee, S., Hwang, C and Moon, JM 2020, “Policy learning and crisis policy-making: quadruple-loop learning and COVID-19 responses in South Korea”, Policy and Society, vol. 39, no. 3, pp. 363–381, DOI 10.1080/14494035.2020.1785195.

Lencioni, P 2006, “Find a rallying cry”, Leadership Processes and Practices, vol. 41, pp. 41–44.

Levit, A 2018, “Does Your Business Have a Regulatory Compliance Strategy?”, American Express, Apr, pp. 1–7, viewed 27/10/2020, <https://www.americanexpress.com/en-us/business/trends-and-insights/articles/does-your-business-have-a-regulatory-compliance-strategy/>.

Li, Z 2014, “Mutual monitoring and corporate governance”, Journal of Banking & Finance, vol. 45, pp. 255-269, DOI 10.1016/j.jbankfin.2013.12.008, <http://dx.doi.org/10.1016/j.jbankfin.2013.12.008>.

Linden, A & Staples, W 2018, “The way banks are organised makes it hard to hold directors and executives criminally responsible”, The Conversation, <https://theconversation.com/the-way-banks-are-organised-makes-it-hard-to-hold-directors-and-executives-criminally-responsible-93638>.

Maennel, K., Mases and Maennel, O 2018, “Cyber Hygiene: The Big Picture”, Lecture Notes in Computer Science, vol. 11252, DOI 10.1007/978-3-030-03638-6.

Manske, M 2020, “The importance of a CISO”, West Monroe, pp. 1–4, viewed 11/01/2021, <https://www.westmonroepartners.com/perspectives/in-brief/the-importance-of-a-ciso>.

Mardis, RM 2015, “Crisis, Strategy, and Response: Investigating the State of Strategic Leadership in Emergency Management”, School of Public Service Leadership, Capella University, ProQuest Dissertations Publishing.

Massingham, R., Massingham, PR and Dumay, J 2019, “Improving integrated reporting”, Journal of Intellectual Capital, vol. 20, no. 1, pp. 60–82, DOI 10.1108/jic-06-2018-0095.

Maynard, SB., Onibere, M and Ahmad, A 2018, “Defining the Strategic Role of the Chief Information Security Officer”, Pacific Asia Journal of the Association for Information Systems, vol. 10, no. 3, DOI: 10.17705/1pais.10303, <https://aisel.aisnet.org/pajais/vol10/iss3/3/>.

Maynard, SB., Tan, T., Ahmad, A and Ruighaver, T 2018, “Towards a Framework for Strategic Security Context in Information Security Governance”, Pacific Asia Journal of the Association for Information Systems, pp. 65–88, DOI 10.17705/1pais.10403.

McClory, S, & Read, M, and Labib, A 2017, “Conceptualising the lessons-learned process in project management: Towards a triple-loop learning framework”, International Journal of Project Management, vol. 35, no. 7, Sep, pp. 1322–1335, DOI 10.1016/j.ijproman.2017.05.006.

McDonald, C 2016, “Surviving the rise of cybercrime: a non-technical executive guide”, MailGuard, South Melbourne, Victoria, viewed 20/01/2019, <https://www.mailguard.com.au/hubfs/eBook%20Campaign%202017/4991%20Mailguard%20Surviving%20the%20rise%20of%20cybercrime-digital-FA.pdf>.

McKnight, DH & Chervany, NL 2006, “Reflections on an initial trust-building model”, Handbook of trust research, Edward Elgar Publishing pp. 29–51, <https://doi.org/10.4337/9781847202819.00008>.

McLeod, PL 1992, “Are Human-Factors People Really So Different - Comparisons of Interpersonal Behavior and Implications for Design Teams”, Journal of Management Information Systems, vol. 9, no. 1, pp. 113–132, DOI 10.1080/07421222.1992.11517950.

Meier, JD 2011, “Deepak Chopra on the Soul of Leadership”, Sources of Insight, Nov, pp. 1–6, viewed 11/11/2020, <http://sourcesofinsight.com/deepak-chopra-on-the-soul-of-leadership/>.

Meintjes, C & Niemann-Struweg, I 2009, “The role of a professional body in professionalisation: The South African public relations case”, PRism, Public Relations Review, vol. 6, no. 2, Jan, pp. 1–14, <http://praxis.massey.ac.nz/prism_on-line_journ.html>.

Mento, A., Jones, R and Dirndorfer, W 2002, “A change management process: Grounded in both theory and practice”, vol. 3, pp. 45–59, DOI: 10.1080/714042520.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C and Giannakopoulos, G 2014, “The Human Factor of Information Security: Unintentional Damage Perspective”, Procedia – Social and Behavioral Sciences, vol. 147, pp. 424–428, DOI 10.1016/j.sbspro.2014.07.133, <https://doi.org/10.1016/j.sbspro.2014.07.133>.

Miklai, M 2018, “Roles and Skills of the Chief Information Security Officer of a Large Bank in the United States: A Qualitative Single Case Study”, School of Business and Technology, Capella University, ProQuest Dissertations Publishing.

Mishra, S 2015, “Organizational objectives for information security governance: a value focused assessment”, Information & Computer Security, vol. 23, no. 2, Jun, pp. 122–144, DOI 10.1108/ics-02-2014-0016.

MIT Technology Review 2016, “Containing the Career Impact of Cybercrime”, MIT Technology Review, pp. 1–13, viewed 20/12/2021, <https://www.technologyreview.com/2016/07/05/158986/containing-the-career-impact-of-cybercrime/>.

Moore, JF 1993, “Predators and Prey: A New Ecology of Competition”, Harvard Business Review, vol. 71, no. 3, pp. 75–86.

Moraetes, G 2017, “CISO Complexity: A Role More Daunting Than Ever”, Security Intelligence, Mar, pp. 1–5, viewed 8/01/2021, <https://securityintelligence.com/ciso-complexity-a-role-more-daunting-than-ever/>.

Morgan, N 2020, “Understanding what cyber hygiene is and its importance for your cybersecurity”, Triskele Labs, Oct, pp. 1–4, viewed 2/09/2021, <https://triskelelabs.com/understanding-what-cyber-hygiene-is-and-its-importance-for-your-cybersecurity/>.

Morgan, S 2015, “IBM's CEO on hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World”, Forbes, Nov, pp. 1–3, viewed 9/12/2019, <https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/?s…>.

Moyo, NT 2016, “PAS-Module 4; Functions of a Professional Association”, International Confederation of ... American College of Nurse-Midwives, vol. 05, May, pp. 1–9, viewed 17/04/2019, <http://www.strongprofassoc.org/wp-content/uploads/2016/05/PAS-Module-4-May2016.pdf>.

MRH 2015, “How to Overcome Your Predecessor”, The Manager’s Resource Handbook (MRH), Apr, pp. 1–8, viewed 1/04/2021, <https://www.managersresourcehandbook.com/how-to-overcome-your-predecessor/>.

Nambisan, S 2018, “Architecture vs. ecosystem perspectives: Reflections on digital innovation”, Information and Organization, vol. 28, no. 2, May, pp. 104–106, viewed Jun, DOI 10.1016/j.infoandorg.2018.04.003.

NETJMC 2020, “Resistance and Insistence – Opposing Forces”, NETJMC – The New Era Workplace Shift, Jul, pp. 1–9, viewed 20/02/2021, <https://www.netjmc.com/resistance-and-insistence-opposing-forces/>.

Nicolini, D 2012, “Chapter 1: Introduction”, in Practice theory, work, and organization: An introduction., OUP Oxford.

NIH 2019, “Definition of COVID-19”, National Cancer Institute(NIH), viewed 20/03/2021, <https://www.cancer.gov/publications/dictionaries/cancer-terms/def/covid-19>.

NIST 2019a, “Success Story: University of Pittsburgh”, NIST, Feb, pp. 1–4, viewed 15/04/2019, <https://www.nist.gov/cyberframework/success-stories/university-pittsburgh>.

NIST 2019b, “Success Story_ Multi-State – Information Sharing and Analysis Center”, NIST, no. 2423, Feb, pp. 1–4, viewed 15/04/2019, <https://www.nist.gov/cyberframework/success-stories/ms-isac>.

NormShield 2019, “Supply Chain Cyber Risk are Finally Part of the NIST Cybersecurity Framework”, NormShield Cyber Risk Scorecard, June 4, viewed:

19/03/2019, <https://www.normshield.com/supply-chain-cyber-risk-are-finally-part-of-the-nist-cybersecurity-framework/>.

Nourse, S 2017, “Why CIOS Cannot Be Solely Responsible For Cybersecurity”, Internet Solutions, May 9, Accessed: 5/08/2019, <https://www.is.co.za/blog/articles/why-cios-cannot-be-solely-responsible-for-cybersecurity-tofu/>.

Nova Systems 2019, Information & Cyber Security, viewed: 5/12/2019, <https://www.novasystems.com/markets/joint/>.

OAIC 2020, “Notifiable Data Breaches Report”, The Office of the Australian Information Commissioner (OAIC), Australian Government, Jul, pp. 1–29, viewed 12/08/2020, <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2020/>.

Oppong, SA., Yen, DC and Merhout, JW 2005, “A new strategy for harnessing knowledge management in e-commerce”, Technology in Society, vol. 27, no. 3, pp. 413–435, DOI 10.1016/j.techsoc.2005.04.009.

Parsons, K., McCormac., Butavicius, M., Pattinson, M and Jerram, C 2013, “The development of the human aspects of information security questionnaire (HAIS-Q)”, in Hepu Deng & Craig Standing (ed.)' ACIS 2013: Information systems: transforming the future: Proceedings of the 24th Australasian Conference on Information Systems, Melbourne, Australia, pp. 1–11.

Patnayakuni, R & Patnayakuni, N 2014, “Information Security in Value Chains: A Governance Perspective, A Governance Perspective Information Security in Value Chains, AMCIS”, paper presented at Twentieth Americas Conference on Information Systems, Savannah.

Pattinson, M & Jerram, C 2013, “A study of information systems risk perceptions at a local government organisation”, in Hepu Deng & Craig Standing (eds), Proceedings of the 24th Australasian Conference on Information Systems (ACIS), Melbourne, Australia, vol. 4, pp. 1–11.

Pearce, R 2018, “APRA issues new cyber security standard for banks”, COMPUTERWORLD, Nov, pp. 1–6, viewed 4/12/2019, <https://www.computerworld.com.au/article/649269/apra-issues-new-cyber-security-standard-banks/>.

Peng, S 2018, "'Private' Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime", Cornell International Law Journal, vol. 51, no. 2, Artic 4, Spring, pp. 445–470, viewed 20/10/2019, <https://scholarship.law.cornell.edu/cilj/vol51/iss2/4>.

Pettigrew, JA, III 2012, "Decision-making by effective information security managers", School of Engineering and Applied Sciences, Ann Arbor thesis, The George Washington University.

Pfeiffer, Y & Wehner, T 2012, "Incident Reporting Systems in Hospitals: How Does Learning Occur Using this Organisational Instrument?", BMJ, vol. 320, no. 7237, Mar 18, pp. 759–763.

Pompon, R 2017, "CIO or C-Suite: To Whom Should the CISO Report? ", F5, Jul, pp. 1–5, viewed 11/5/2019, <https://www.darkreading.com/partner-perspectives/f5/cio-or-c-suite-to-whom-should-the-ciso-report/a/d-id/1329807>.

Porter, ME 1980, Competitive Strategy: Techniques for Analyzing Industries and Competitors., The Free Press, New York.

Potter, LE & Vickers, G 2015, "What Skills do you Need to Work in Cyber Security?", paper presented at Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research ACM, pp. 67–72.

Press, G 2015, "Why Your Company's Next CEO Is Not Your Current CIO", Forbes, Feb, pp. 1–4, viewed 24/09/2021, <https://www.forbes.com/sites/gilpress/2015/02/18/why-your-companys-next-ceo-is-not-your-current-cio/?sh=1195253d1da1>.

Proctor, RW, & Lien, M-C, & Schultz, EE, and Salvendy, G 2000, "Human Factors in Information Security Methods", Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 44, no. 2, pp. 357–357 DOI 10.1177/154193120004400219.

Protiviti Australia 2019, "Board Oversight of Cyber Risk, pp. 1–9, viewed 3/4/19, <https://www.protiviti.com/AU-en/insights/bpro90>.

PwC 2021, "2022 Global Digital Trust Insights Survey – PwC", pp. 1–31, viewed 10/12/2021, <https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html.>.

Pye, G., Warren, M., Salzman, S., van der Meer, R., AustCyber and Cynch Security 2021, “Big cyber security questions for small business The state of cyber fitness in Australian small businesses”, Cynch Security, Feb, pp. 1–40, viewed 24/02/2021, <https://cynch.com.au/s/Cynch-Big-cyber-security-questions-for-small-business-White-paper-bjs5.pdf>.

Quigley, K., Burns, C and Stallard, K 2015, “‘Cyber Gurus’: A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection”, Government Information Quarterly, vol. 32, no. 2, Apr, pp. 108–117, DOI 10.1016/j.giq.2015.02.001, < http://dx.doi.org/10.1016/j.giq.2015.02.001>.

Raghu, A 2018, “A Comparison of Cyber Security Regulation in the USA and Australia”, Hivint, May 28, Accessed: 14/02/2019, <https://blog.hivint.com/a-comparison-of-cyber-security-regulation-in-the-usa-and-australia-5bdeb5c4c2df>.

Rattray, G., Gijsbers, K., Tikk, E., Purdy, A., Mulvenon, J and Carr, J 2011, “Panel_2_Cyber security, economics, and a healthier ecosystem”, Georgetown Journal of International Affairs.

Reed, CGE 2006, “Leadership and Systems Thinking Defence”, Defense AT&L, May-June, pp. 10–13, viewed 11/10/20, <https://www.dau.edu/library/defense-atl/DATLFiles/2006_05_06/ree_mj06.pdf>.

Reeder, FS 2014, “The Case for Professionalizing Cybersecurity”, FedTech Magazine, Apr, pp. 1–5, viewed 3/05/2019, <https://fedtechmagazine.com/article/2014/04/case-professionalizing-cybersecurity>.

Relihan, T 2019, “These are the cyberthreats lurking in your supply chain”, MIT Sloan, Feb, pp. 1–6, viewed 3/11/2019, <http://mitsloan.mit.edu/ideas-made-to-matter/these-are-cyberthreats-lurking-your-supply-chain>.

Reynolds, DD & Tamburello, LM 2016, “Cybersecurity Madness: 3 Things that Really Matter and 3 That Don't”, Corporate Counsel, Nov, pp. 1–3, viewed 10/11/2020, <https://www.mdmc-law.com/articles/cybersecurity-madness-3-things-really-matter-and-3-things-dont-corporate-counsel-november>.

Richards, K 2018, “3 Questions for Better Supply Chain Cybersecurity”, Marsh, Sep, pp. 1–3, viewed 3/12/2019, <https://www.marsh.com/us/insights/risk-in-context/three-questions-for-better-supply-chain-cybersecurity.html>.

Robert-Edomi, S 2014, “CBI demands action on growing skills vacuum”, Training Journal(TJ), Mar, pp. 1–6, viewed 11/19/2020, <https://www.trainingjournal.com/articles/news/cbi-demands-action-growing-skills-vacuum>.

Rogelberg, D 2016, “The New CISO: From Technology to Business Focused Leadership, 25 CISOs Share Expert Advice on How to Make it in the C Suite”, Mighty Guides Sponsored Fortinet, Aug, pp. 1–61, viewed 30/11/2020, <https://mightyguides.com/wp-content/uploads/2018/08/Fortinet_ebook_THENEWCISO_final.pdf>.

Rosenbaum, E 2021, “Microsoft has a $20 billion hacking plan, but cybersecurity has a big spending problem”, CNBC, Sep, pp. 1–9, viewed 10/10/2021, <https://www.cnbc.com/2021/09/08/microsofts-20-billion-and-cybersecuritys-big-spending-problem.html>.

Rosenquist, M 2018, “Cybersecurity Fails Without Strategy”, BBN Times, Nov, pp. 1–19, viewed 16/01/2021, <https://www.bbntimes.com/technology/cybersecurity-fails-without-strategy>.

Roy, D & Zeckhauser, R 2015, “Anatomy of Ignorance: Diagnoses from Literature”, in IMGLM (Eds.) (ed.), Routledge International Handbook of Ignorance Studies, Routledge, Oxford, England, pp. 61–72, DOI 10.4324/9781315867762-8, <https://scholar.harvard.edu/files/rzeckhauser/files/anatomy_of_ignorance.pdf>.

RSI Security 2019, “Why Is Cyber Hygiene Important”, RSI Security, 23/09/2020, < https://blog.rsisecurity.com/why-is-cyber-hygiene-important/#:~:text=Defining Cyber Hygiene&text=This means protecting and maintaining,now an…>.

Ruiz, D 2020, “The cybersecurity skills gap is misunderstood”, Malwarebytes Labs, August 25, Accessed: 9/11/2020, <https://blog.malwarebytes.com/business-2/2020/08/the-cybersecurity-skills-gap-is-misunderstood/>.

Ryan, P 2019, “Review slams APRA for keeping a low profile, urges overhaul of the regulator”, ABC News (Australian Broadcasting Corporation), Jul, pp. 1–2, viewed 11/04/2019, <https://www.abc.net.au/news/2019-07-17/review-urges-overhaul-of-apra-after-banking-royal-commission/11315510>.

Sadowski, G 2020, “CISO Liability and Lawsuits in the Face of a Crisis, Part 2”, Meduim, Dec, pp. 1–7, viewed 22/12/2021, <https://www.exabeam.com/security-operations-center/ciso-liability-and-lawsuits-in-the-face-of-a-crisis-part-2/>.

Sainty Law 2017, “Cybersecurity: The Regulatory Environment”, saintylaw, Mar, pp. 1–7, viewed 25/03/2019, <http://www.saintylaw.com.au/2017/03/21/cyber-security-regulatory-environment/>.

Salimath, MS & Philip, J 2020, “Cyber management and value creation: an organisational learning-based approach”, Knowledge Management Research & Practice, vol. 18, no. 4, pp. 474-487, DOI 10.1080/14778238.2020.1730719.

Schrank, M & Young, RB 1987, “The role of professional associations”, New directions for student services, Germantown, NY: Wiley Subscription Services, Inc., A Wiley Company, vol. 1987, no. 37, pp. 61–68, viewed Spring DOI 10.1002/ss.37119873708.

Secureworks 2017, “Cyber Threat Basics, Types of Threats, Intelligence & Best Practices”, Secureworks, May 12, Accessed: 4/03/2019, <https://www.secureworks.com/blog/cyber-threat-basics>.

Seeholzer, RV 2015, “Investigating Roles of Information Security Strategy”, Dissertation, Nova Southeastern University, ProQuest Dissertations Publishing.

Seo, M-G 2003, “Overcoming Emotional Barriers, Political Obstacles, and Control Imperatives in the Action-Science Approach to Individual and Organizational Learning”, Academy of Management learning & education, vol. 2, no. 1, p. 7–21, DOI 10.5465/AMLE.2003.9324011.

Shreeve, B., Hallett, J., Edwards, M., Ramokapane, KM., Atkins, R and Rashid, A 2020, “The best laid plans or lack thereof: Security decision-making of different stakeholder groups”, IEEE Transactions on Software Engineering, pp. 1–13, DOI 10.1109/tse.2020.3023735.

Snell, R & Chak, AM-K 1998, “The learning organization: Learning and empowerment for whom?”, Management Learning, vol. 29, no. 3, pp. 337–364, DOI 10.1177/1350507698293005.

SolarWinds n.d., “Security Patch Management”, viewed 30/11/2021, <https://www.solarwinds.com/patch-manager/use-cases/security-patch-management>.

Soundararajan, V, & Brown, JA, and Wicks, AC 2019, “Can Multi-Stakeholder Initiatives Improve Global Supply Chains? Improving Deliberative Capacity with a Stakeholder Orientation”, Business Ethics Quarterly, vol. 29, no. 3, Jul, pp. 385–412, viewed 20/10/2019, DOI 10.1017/beq.2018.38.

Stackpole, B 2017, “Is Your Firm Resting on its Security Laurels?”, Symantec, Accessed : 28/11/2019, <https://www.symantec.com/blogs/feature-stories/your-firm-resting-its-security-laurels>.

Stark, JR 2017, “Top Cybersecurity Concerns for Every Director”, Corporate Governance Advisor, vol. 25, no. 2, pp. 1–10.

Stilgherrian 2015, “Why is hacking so easy and security so hard?”, ABC Radio National (Australian Broadcasting Corporation), Dec, pp. 1–7, viewed 22/08/2019, <https://www.abc.net.au/radionational/programs/futuretense/what-makes-hacking-so-easy-and-security-so-hard/6990902>.

Stilgherrian 2019, “ACSC dumps annual conference, partners with AISA for cyber events”, ZDNET, Jan, pp. 1–5, viewed 29/01/2021, <https://www.zdnet.com/article/acsc-dumps-annual-conference-partners-with-aisa-for-cyber-events/>.

Stryve 2020, “Legal and Regulatory Elements of a CISO’s Role”, Accessed: 23/10/2020, <https://www.stryvesecure.com/blogs/legal-and-regulatory-elements-of-a-cisos-role >.

Suddaby, R., Bévort, F and Strandgaard Pedersen, J 2019, “Professional judgment and legitimacy work in an organizationally embedded profession”, Journal of Professions and Organization, vol. 6, no. 2, Jul, pp. 105–127, DOI 10.1093/jpo/joz007, <https://doi.org/10.1093/jpo/joz007>.

Sushanta, KS 2017, “Theorization of New Practices in Emerging Organizational Fields”, Vikalpa:Journal for Decision Makers, vol. 42, no. 3, Aug, pp. 131–144, DOI 10.1177/0256090917719980, <https://doi.org/10.1177/0256090917719980>.

Tan, A 2020, “Cyber security is next frontier for open source”, Computer Weekly, Sep, pp. 1–6, viewed 24/11/2020, <https://www.computerweekly.com/news/252488909/Cyber-security-is-next-frontier-for-open-source>.

Tan, TCC., Ruighaver, AB and Ahmad, A 2010, “Information Security Governance: When Compliance Becomes More Important than Security”, in SEC., Springer Berlin Heidelberg, Berlin, Heidelberg, vol. 330, pp. 55–67.

Tanium in partnership with NASDAQ - UPGUARD 2016, “EXECUTIVE FALLOUT FROM CYBERCRIME: LAWSUITS AND CAREER DAMAGE”, UPGUARD.COM, viewed 23/10/19, <https://www.yumpu.com/en/document/view/55848146/executive-fallout-from-cybercrime-lawsuits-and-career-damage>.

Tankard, C 2016, “What the GDPR means for businesses”, Network Security, vol. 2016, no. 6, Jun, pp. 5–8, viewed 5/05/2019, DOI 10.1016/s1353-4858(16)30056-3, <https://doi.org/10.1016/S1353-4858(16)30056-3.>.

TAT 2019, “Data Decryption Bill Vulnerable to Hacking?”, The Australian Tribute, Mar, pp. 1–9, viewed 4/03/2019, <https://www.theaustraliantribune.com.au/2019/03/data-decryption-bill-vulnerable-to-hacking/>.

Tebbs, P 2019, “Got a Frankenstack? Why Piecemeal Isn’t Scalable When Selling Software Online”, Paddle, June 10, Accessed: 24/11/2020, <https://paddle.com/blog/frankenstack-why-piecemeal-isnt-scalable/>.

Thomas, LDW & Autio, E 2014, “The Fifth Facet: The Ecosystem as an Organizational Field'', paper presented at Academy of Management Proceedings 2,014-01, Vol.2014 (1), p.10306, DRUID Society Conference 2014, CBS, Copenhagen, June 16-18.

Thomson Reuters 2018, “Combating cybercrime: does the law need to catch up? Legal Insights Europe”, Thomson Reuters, May 14, Accessed: 1/04/2019, <https://blogs.thomsonreuters.com/legal-uk/2018/05/14/wicombatting-cybercrime-does-the-law-need-to-catch-up/>.

Thycotic 2019, “2019 Cyber Security Teams Survey Report; The CISO Challenge:; Aligning Business Enablement with Enforcement”, Thycotic, pp. 1–14, viewed 20/02/2020, <https://thycotic.com/resources/cyber-security-executives-survey-report-europe/>.

Timmermans, K., Roark, C and Abdalla, R 2019, The Big Zero: The Transformation of ZBB into a Force for Growth, Innovation and Competitive Advantage Penguin, UK.

Tisdale, SM 2016, “Architecting A Cybersecurity Management Framework: Navigating And Traversing Complexity, Ambiguity, And Agility', Robert Morris University.

Tokar, S 2020, “Types of Cyber Security Roles: Job Growth and Career Paths”, SNHU, Jul, pp. 1–8, viewed 10/09/2021, <https://www.snhu.edu/about-us/newsroom/2020/07/cyber-security-roles>.

Tosey, P 2005, “The Hunting of the Learning Organization: A Paradoxical Journey”, Management Learning, vol. 36, no. 3, Sep, pp. 335–352.

Tosey, P., Visser, M and Saunders, MNK 2011, “The origins and conceptualizations of ‘triple-loop’ learning: A critical review”, Management Learning, vol. 43, no. 3, pp. 291–307, DOI 10.1177/1350507611426239.

Towers-Clark, C 2018, “Relaxed, Anxious, Ignorant: Our Attitudes Towards CyberSecurity Are Making The Problem Worse”, *Forbes*, Nov, pp. 1–5, viewed 20/12/2020, <https://www.forbes.com/sites/charlestowersclark/2018/11/09/relaxed-anxious-ignorant-our-attitudes-towards-cybersecurity-are-making-the-problem-worse/>.

Townsend, K 2018, “Professionalizing Cybersecurity Practitioners”, Security Week, Sep, pp. 1–9, viewed 30/04/2019, <https://www.securityweek.com/professionalizing-cybersecurity-practitioners-0>.

Tsui, AS., Zhang, Z-X., Wang, H., Xin, KR and Wu, JB 2006, “Unpacking the relationship between CEO leadership behavior and organizational culture”, The Leadership Quarterly, vol. 17, no. 2, Apr, pp. 113–137, DOI 10.1016/j.leaqua.2005.12.001, <https://doi.org/10.1016/j.leaqua.2005.12.001>.

Tucci, L & Roy, M 2019, “Why a CISO-CIO reporting structure undermines security”, Techtarget, Nov, pp. 1–6, viewed 12/10/2019, <https://searchcio.techtarget.com/feature/Why-a-CISO-CIO-reporting-structure-undermines-security>.

Tunggal, AT 2020, “What is Cyber Hygiene and Why is it Important?”, upguard, <https://www.upguard.com/blog/cyber-hygiene>.

Tversky, A & Kahneman, D 1974, “Judgment under uncertainty: Heuristics and biases”, Science., vol. 185, no. 4157, pp. 1124–1131.

USYD 2019, “Professional associations, Engage with your industry and grow your professional network”, Careers Centre. The University of Sydney(USYD), pp. 1–5, viewed 1/05/2019, <https://sydney.edu.au/careers/students/career-advice-and-development/professional-associations.html>.

Visentin, L 2021, “Telstra boss says company directors should be liable for ‘egregious’ cyber-security negligence”, The Sydney Morning Herald, Jul, pp. 1–3, viewed 24/09/2021, <https://www.smh.com.au/politics/federal/most-australian-businesses-under-prepared-for-a-cyber-attack-report-20210715-p589xo.html>.

Von Solms, B & Von Solms, R 2018, “Cybersecurity and information security – what goes where?”, Information and Computer Security, vol. 26, no. 1, pp. 2–9, DOI 10.1108/ICS-04-2017-0025, <http://dx.doi.org/10.1108/ICS-04-2017-0025>.

Von Solms, B 2006, “Information Security – The Fourth Wave”, Computers & Security, vol. 25, no. 3, 165, pp. 165–168, DOI 10.1016/j.cose.2006.03.004.

Von Solms, R & Van Niekerk, J 2013, “From information security to cyber security”, Computers & Security, vol. 38, pp. 97–102.

Von Solms, R & Von Solms, SHB 2006, “Information security governance: Due care”, Computers & Security, vol. 25, no. 7, pp. 494–497, DOI 10.1016/j.cose.2006.08.013.

Waal, Ad., Weaver, M., Day, T and Heijden, Bvd 2019, “Silo-Busting: Overcoming the Greatest Threat to Organizational Performance”, Sustainability, vol. 11, no. 23, 6860, viewed 03/05/2021, DOI 10.3390/su11236860.

Wang, G, & Holmes, RM, & Oh, I-S, and Zhu, W 2016, “Do CEOs Matter to Firm Strategic Actions and Firm Performance? A Meta-Analytic Investigation Based on Upper Echelons Theory”, Personnel Psychology, vol. 69, no. 4, pp. 775–862, DOI 10.1111/peps.12140.

Warner, J 2005, “Multi-stakeholder platforms: integrating society in water resource management?”, Ambiente & Sociedade, vol. 8, no. 2, July/Dec, pp. 4–28, DOI 10.1590/s1414-753x2005000200001, <https://doi.org/10.1590/S1414-753X2005000200001>.

Weishäupl, E., Yasasin, E and Schryen, G 2015, “A Multi-Theoretical Literature Review on Information Security Investments using the Resource-Based View and

the Organizational Learning Theory", paper presented at Thirty Sixth International Conference on Information Systems, Fort Worth 2015 (ICIS).

Westby, JR & Allen, JH 2007, "Governing for Enterprise Security (GES) Implementation Guide", Software Engineering Institute,U.S. Department of Defense, Aug, pp. 1–116, viewed 13/04/2021, <https://resources.sei.cmu.edu/asset_files/TechnicalNote/2007_004_001_14837.pdf>.

White, D 2018, "How Cybersecurity is Beneficial for HR Professionals", TechFunnel, Sep, pp. 1–4, viewed 20/12/2018, <https://www.techfunnel.com/hr-tech/how-cybersecurity-is-beneficial-for-hr-professionals/>.

Wild, J 2018, "Five Most Common Security Frameworks Explained", Origin IT, Mar, pp. 1–6, viewed 12/04/2019, <https://originit.co.nz/the-strongroom/five-most-common-security-frameworks-explained/>.

Williams, P 2007, "Executive and board roles in information security", Network Security, vol. 2007, no. 8, 11, pp. 11–14, DOI 10.1016/s1353-4858(07)70073-9.

Winder, D 2019, "The voice of risk: how CISOs can make themselves heard", Raconteur, pp. 1–13, viewed 27/10/2019, <https://www.raconteur.net/technology/ciso-risk-board>.

Wolff, J 2016, "Perverse Effects in Defense of Computer Systems: When More Is Less", Journal of Management Information Systems, vol. 33, no. 2, pp. 597–620.

Worstell, K 2018, "Cybersecurity Burnout: What it Is, Why It Matters, and What to Do About It", LinkedIn, Nov, pp. 1–7, viewed 3/09/2019, <https://www.linkedin.com/pulse/cybersecurity-burnout-what-why-matters-do-karen-worstell-ma-ms/>.

Zacharias, NA., Six, B., Schiereck, D and Stock, RM 2015, "CEO influences on firms' strategic actions: A comparison of CEO-, firm-, and industry-level effects", Journal of Business Research, vol. 68, no. 11, pp. 2338–2346, DOI 10.1016/j.jbusres.2015.03.045, <http://dx.doi.org/10.1016/j.jbusres.2015.03.045>.

Zardini, A., Rossignoli, C and Ricciardi, F 2016, "A bottom-up path for IT management success: From infrastructure quality to competitive excellence",

Journal of Business Research, vol. 69, no. 5, May, pp. 1747–1752, DOI 10.1016/j.jbusres.2015.10.049, <https://doi.org/10.1016/j.jbusres.2015.10.049>.

Zhang, C., Xue, L and Dhaliwal, J 2016, “Alignments between the depth and breadth of inter-organizational systems deployment and their impact on firm performance”, Information & Management, vol. 53, no. 1, pp. 79–90.

Zimmermann, A., Oshri, I., Lioliou, E and Gerbasi, A 2018, “Sourcing in or out: Implications for social capital and knowledge sharing”, Journal of Strategic Information Systems, vol. 27, no. 1, Mar, pp. 82–100, DOI 10.1016/j.jsis.2017.05.001, <http://dx.doi.org/10.1016/j.jsis.2017.05.001>.

Zongo, P 2019, “Positioning the CISO to Succeed”, CSO, Aug, pp. 1–6, viewed 11/5/2019, <https://www.cso.com.au/article/665166/positioning-ciso-succeed/>.

Zook, C 2016, “Maintaining Your Focus on the Front Lines as Your Company Grows”, Harvard Business Review, Sep, pp. 2–5, viewed 24/10/2019, <https://hbr.org/2016/09/maintaining-your-focus-on-the-front-lines-as-your-company-grows>.

APPENDICES

Appendix A: Phase 1. Resource rigour: ranking of cited references

Table A. 1 – Journals listed in the Financial Times (FT List) with ABDC ranking of A* and A

Journal	*No*	*Ranking*
Academy of Management Journal	*12*	*A**
Academy of Management Review	*4*	*A**
Accounting, Organizations and Society	*4*	*A**
Administrative Science Quarterly	*5*	*A**
Human Relations	*1*	*A**
Human Resource Management	*3*	*A**
Information Systems Research	*3*	*A**
Journal of Management	*10*	*A**
Journal of Management Information Systems	*29*	*A**
Journal of Management Studies	*1*	*A**
Journal of Operations Management	*1*	*A**
Management Science	*3*	*A**
MIS Quarterly	*27*	*A**
Organization Science	*5*	*A**
Organization Studies	*3*	*A**
Organizational Behavior and Human Decision Processes	*15*	*A**
Strategic Management Journal	*1*	*A**
Harvard Business Review	*28*	*A*
Journal of Applied Psychology	*4*	*A*
Journal of Business Ethics	*1*	*A*
MIT Sloan Management Review	*2*	*A*

Table A. 2 – ABDC ranking of A* (not included in FT ranking)

Journal	No	Ranking
Academy of Management Learning and Education	1	A*
ACM Transactions on Computer-Human Interaction	1	A*
American Psychologist	1	A*
Decision Sciences	1	A*
Decision Support Systems	20	A*
European Journal of Information Systems	2	A*
European Journal of Marketing	1	A*
European Journal of Operational Research	1	A*
Industrial Marketing Management	1	A*
Information and Management	14	A*
Information and Organization	14	A*
International Journal of Hospitality Management	1	A*
International Journal of Production Economics	1	A*
Journal of Banking and Finance	11	A*
Journal of Economic Behavior and Organization	1	A*
Journal of Organizational Behavior	1	A*
Journal of Strategic Information Systems	13	A*
Management Accounting	1	A*
Personnel Psychology	1	A*
The Leadership Quarterly	32	A*

Table A. 3 – ABDC ranking of A (not included in FT ranking)

Journal	No	Ranking
Academy of Management Executive	*2*	*A*
Accounting and Finance	*1*	*A*
Accounting, Auditing and Accountability Journal	*2*	*A*
Australian Journal of International Affairs	*1*	*A*
British Journal of Sociology	*1*	*A*
California Management Review	*3*	*A*
Communications of the ACM	*6*	*A*
Computers and security	*41*	*A*
Human-computer Interaction	*1*	*A*
IBM Systems Journal	*1*	*A*
Information and Software Technology	*3*	*A*
Information Systems Frontiers	*1*	*A*
Insurance: Mathematics and Economics	*1*	*A*
International Affairs	*1*	*A*
International Journal of Information Management	*9*	*A*
International Journal of Operations and Production Management	*1*	*A*
Journal of Knowledge Management	*7*	*A*
Journal of Accounting and Public Policy	*1*	*A*
Journal of Business Research	*2*	*A*
Journal of the Operational Research Society	*1*	*A*
Journal of World Business	*1*	*A*
Long Range Planning	*1*	*A*
MIS Quarterly Executive	*5*	*A*
Organizational Dynamics	*1*	*A*
Public Administration Quarterly	*2*	*A*
Public Administration Review	*2*	*A*
Public Relations Review	*1*	*A*

Small Group Research	*1*	*A*
Supply Chain Management: An International Journal	*2*	*A*
System Dynamics Review	*2*	*A*
Texas International Law Journal	*1*	*A*
The Journal of Computer Information Systems	*2*	*A*
The Journal of the Operational Research Society	*3*	*A*

Appendix B: Phase 1. Method: Analytical coding

Figure A. 1. Screenshot of a word cloud displaying dominant themes arising in early stages of analysis.

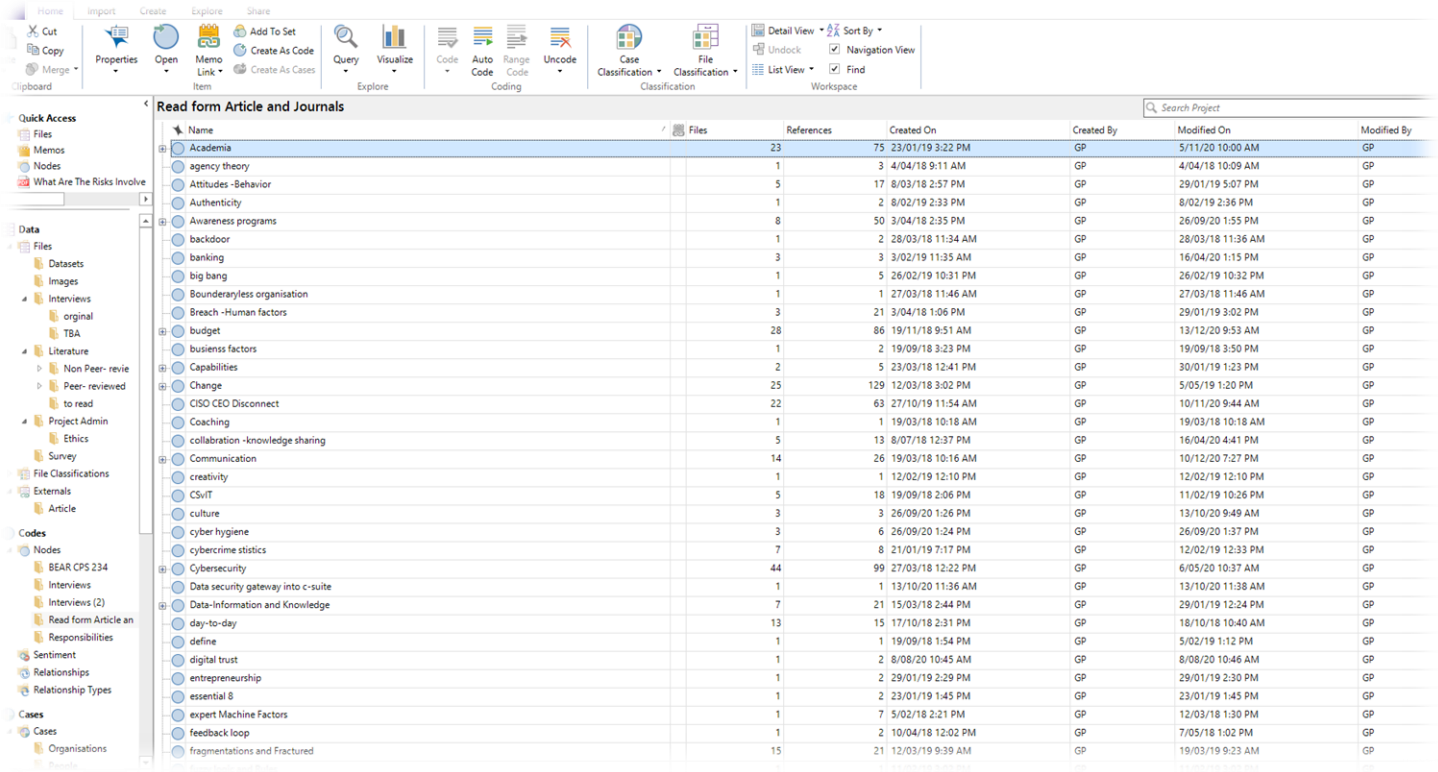

Figure A. 2. Screenshot of first qualitative coding of themes

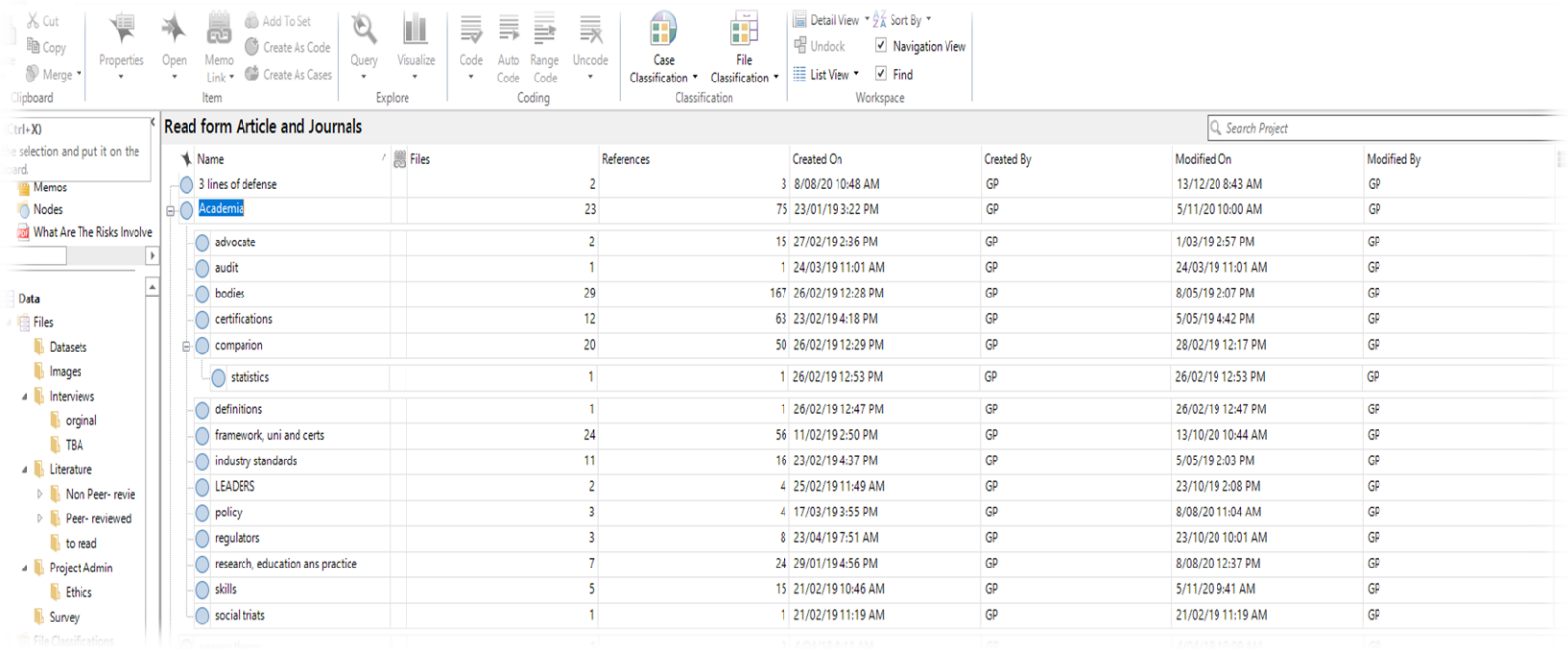

Figure A. 3. Screenshot of second pass identifying key themes

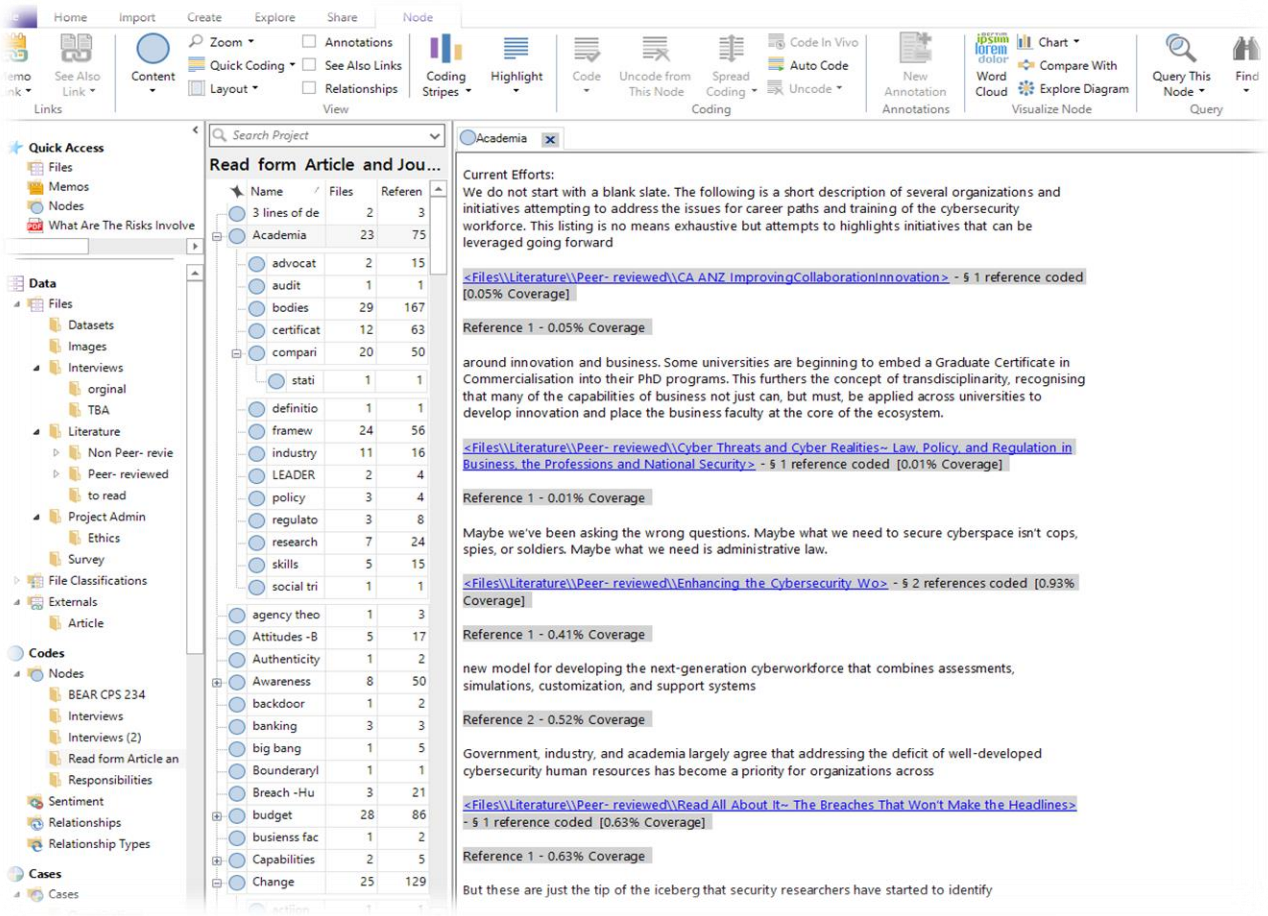

Figure A. 4. Screenshot of code contents with reference source example

Appendix C: Phase 1. Theory: Full depiction of diagrammed theoretical construct

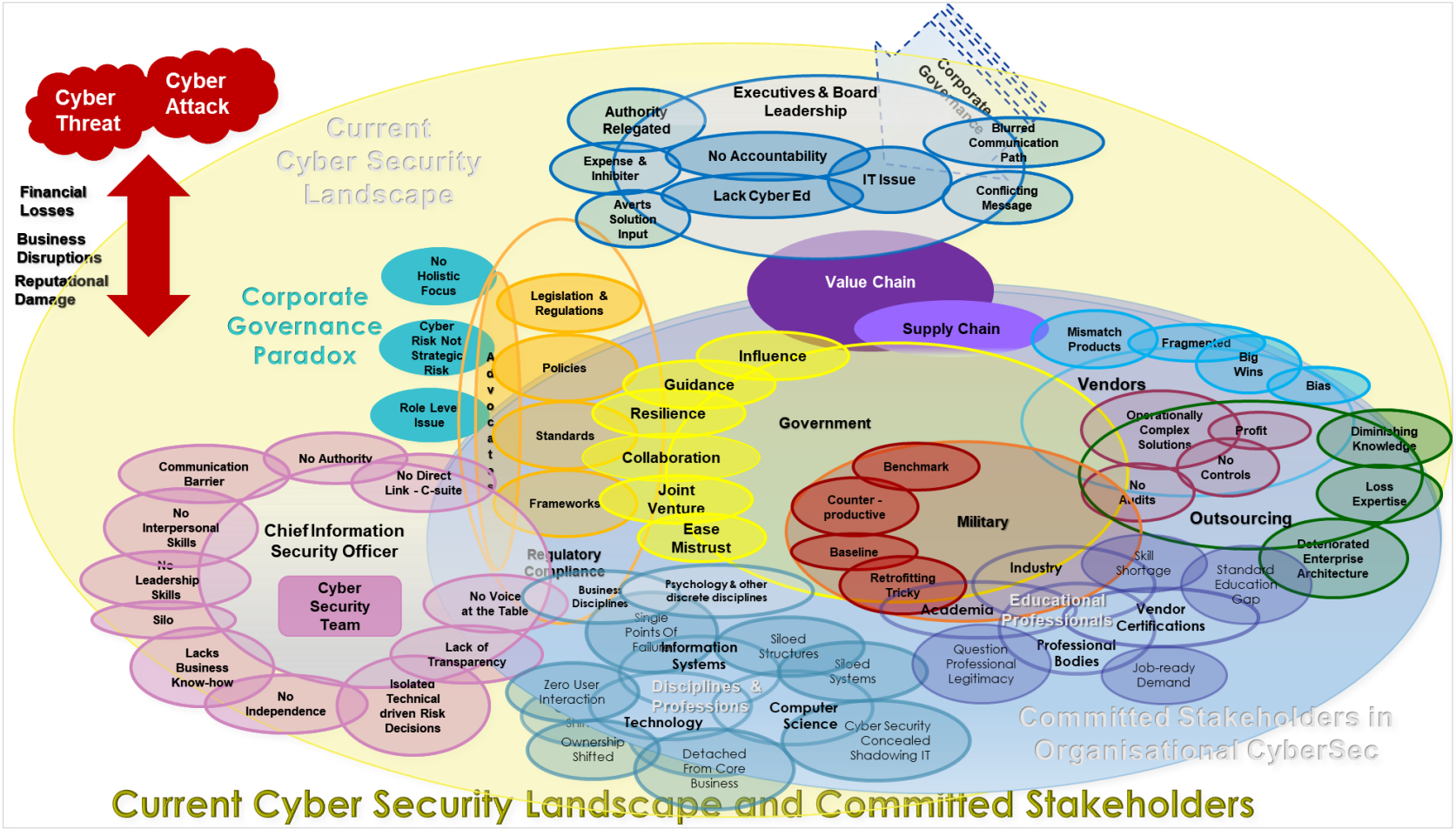

Figure A. 5. Complex model – Current Cyber security Landscape and Committed Stakeholders

As discussed above, following the four passes of analysis, we mapped the results and created models (Figure 4.1 to Figure 4.9) that enable us to perceive each principal stakeholder of organisational cyber security in the context of their interrelationships. This synthesised analysis allows us to understand the current landscape of organisational cyber security and the mapped interrelationships clearly illustrate that the multi-disciplinarity is not yet collaborative or cohesive so prohibits a holistic approach to cyber resilience.

Seen in the context of stakeholder interrelationships, we identified a landscape of fragmented interactions impeded by the overlapping, but dissociated silos as depicted in Figure A. 5. This understanding is incorporated into the complex model Figure A. *5* in the teal-coloured grouping [a] “Fragmentation” (described below). Also arising from the synthesis of our findings the concept/title [b] “Cyber governance paradox” was also incorporated (described below).

The patchwork interrelationship model

The Figure A. 5 “complex model” is composed of each of the disparate models (Figure 4.1 to Figure 4.9) built and discussed throughout the paper. Each of Figures 1–9 is a model that illustrates a specific stakeholder in organisational cyber security. We assembled these disparate models to display how each stakeholder relates to organisational cyber security in purpose and function, and consequently ascertain their interrelationships. Summaries of the single models of the principal stakeholders following along with a discussion about how they come together into this complex model.

Regulatory compliance (Figure 4.1) shows that legislation is underpinned by regulations and is aligned to disparate policies used as building blocks to develop unified standards. Frameworks are devised from the *components mentioned above an*d built specifically to manage and solve a specific problem. Advocates, as illustrated, may specialise in one of these branches. However, the need to know and ability to communicate to others about cyber security plays a critical role in the progress and advancement of the cyber domain.

Stakeholder: Government (Figure 4.2) exposes some key government-led attributes (such as influencing, providing guidance, and collaborating) to define and determine whether or how the government will engage joint venture cyber security. Emphasis on cyber resilience through open dialogue eases mistrust and provides stability.

Stakeholder: Military (Figure 4.3) shows that the military leads in the development of cyber security benchmarks, baselines, and standards. Though military and nonmilitary cyber security needs overlap, military standards are frequently incompatible with culture and practices in commercial and other sectors and are often difficult to retrofit.

Stakeholder: Value and supply chains Figure 4.4) depicts a development of Porter’s value chain model that incorporates the full production process, including the supply chain (B2U 2018). The supply chain extends beyond the enterprise’s boundaries, thus complicating the organisation’s ability to control cyber risk.

Stakeholder/s: Vendors, outsourced providers, and consultants (Figure 4.5) show how these stakeholders are intrinsically linked while coexisting independently. Vendors play an influential role as self-promoted cyber experts, keyed up by big wins, promoting their own products (natural bias) while remaining immune to audits or control. A by-product of outsourcing includes surrendering control over strategic enterprise architecture and the loss of specialised expertise which reduces proper compliance measures, leaving the organisation vulnerable.

Stakeholder/s: Disciplines and sub-disciplines (Figure 4.6) shows that the separate, yet interrelated STEM disciplines are understood to be central, yet do not necessarily interconnect other than in normal patterns. These three macro-disciplines and their sub-disciplines are integral and overlap in some cyber security's core curriculum. Significantly, however, newly recognised critical disciplines such as the various Business and Management fields, and Psychology (particularly sub-disciplines dealing with Social Engineering) and other fields such as Law, Criminology, Political Science and other 'discrete disciplines' are recognised as critical "single points of failure", but not often integrated – held outside the established siloed areas of cyber security management. These institutional silos and lack of core business acumen in the central STEM-based cyber disciplines is a pedagogical vulnerability to the interdisciplinary education and development needed for cyber security.

Stakeholder/s: Professional Industry Bodies

Figure 4.7) portrays that discrete single disciplinary learning, dispersed across numerous stakeholders, impedes the practice's legitimacy. Each silo establishes

a specialist body of knowledge that provides professional competencies essential for meeting the current skill gap. However, as with disciplines, this contributes to the fragmentation of cyber security rather than creating to the cohesive and holistic approach needed.

Stakeholder: Chief Information Security Officer (CISO) (Figure 4.8) depicts that this role lacks leadership, interpersonal, and strategic communication skills. These limitations combined with lack of authority due to the reporting structure allows them no voice or autonomy so leads to isolated technical-driven risk decisions.

Stakeholder/s: Organisational leadership (Figure 4.9) stipulates that the lack of training in and understanding of cyber security, facilitates the conflicting message that cyber risk is a technical problem thus absolving executives of their responsibility and relegating accountability.

Concept group [a] “Fragmentation” labels three dominating concepts arising as issues that become evident when seeing Figure 4.1 to Figure 4.9 in interrelationship as depicted in Figure A. 5 . These three significant findings are No holistic focus; Cyber risk not strategic risk; and Role level issue. Concept [b] “Cyber governance paradox” summarises the dominant issue that is perceived when viewing the conjunction of multiple issues in one collective model. The “Cyber governance paradox” is displayed in the model as the underlying pale yellow elliptical shape that depicts how (the lack of) Corporate governance underlies and reinforces all the other issues.

Appendix D: Phase 2. Mind map question design

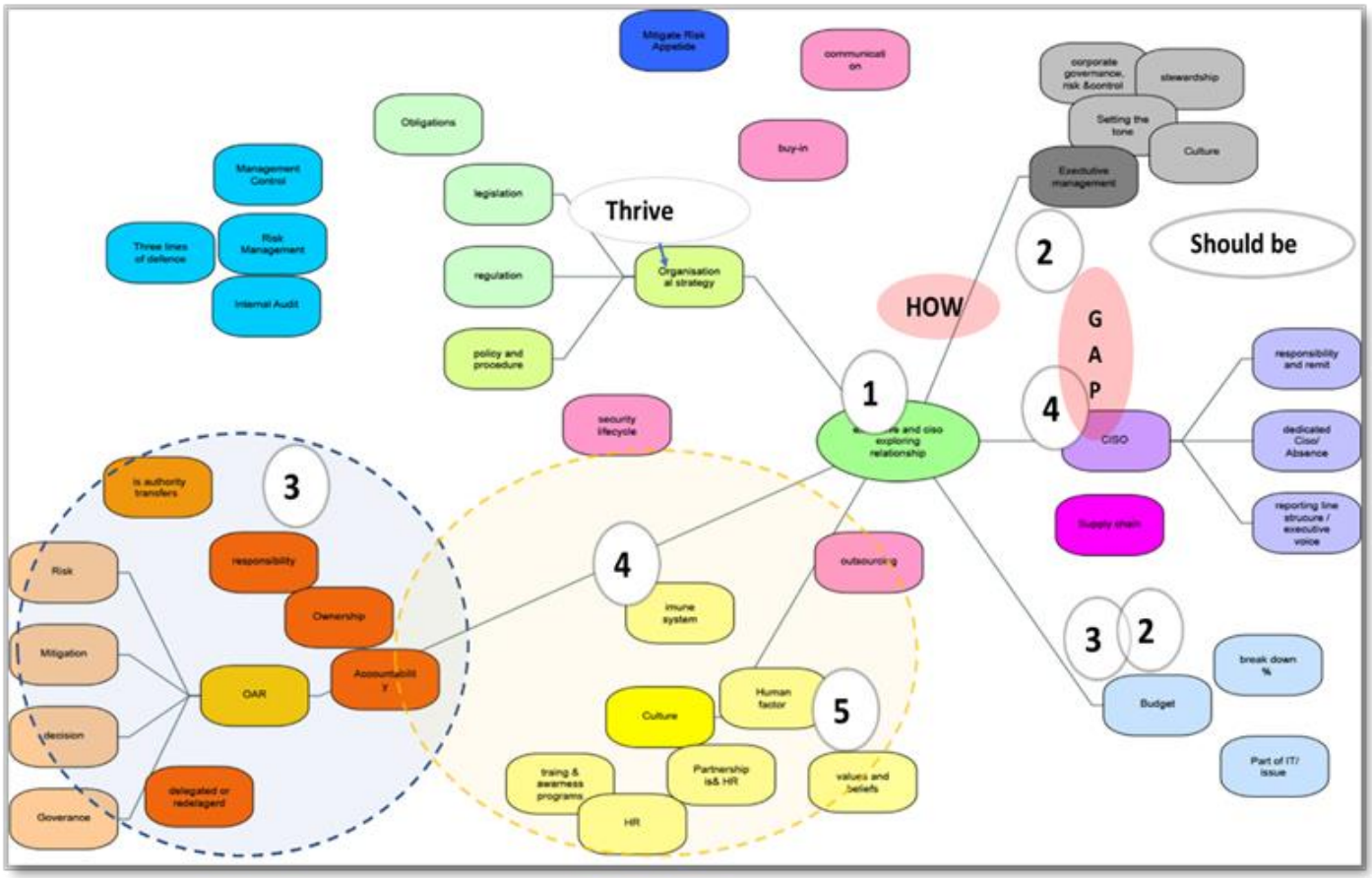

Figure A. 6.Mind map: Designing question for semi-structured interviews

Appendix E: Phase 2. Participants Interview Questions Guide

Thank you for being willing to give us your time… How would you like us to address you?

1. Could you please detail your organisation's cyber security strategy and the resultant policies? (And may we have a copy of your cyber security strategy and policies, please?)
2. What role does the executive management team play in overseeing corporate governance and controls? Do they take an active role in advocating cyber security initiatives to keeping the organisation cyber secure?
3. How has the responsibility assignment matrix of OAR (Ownership, Accountability, Responsibility) been defined for cyber security risk, mitigation decision strategies and governance?
4. What are your responsibilities and specifically in terms of cyber security?
5. How would you describe the cyber security culture in your organisations?
6. Does your organisation have a Chief Information Security Officer (CISO) – i.e.: someone dedicated to your cyber security mission and function?
7. Is your organisational budget structured to embed cyber security as priority?
8. Is there anything important about cyber security in your information that you think we haven't discussed, or needs further discussion or explanation?

Thank you so much for your time – you have been incredibly helpful, and your answers are really valuable to our research.

When we are reviewing and collating the data captured in this interview may we contact you by phone or email to clarify or follow up?

PROBES: INTERNAL USE ONLY

Q1:

a. How does your strategy meet your legislative and regulatory obligations?
b. What policies and procedures are in place to help to mitigate your risk appetite?
c. How do these policies reflect regulatory compliance and the organisation's objectives for security?

Q4:

a. What are you accountable for?
b. Are there responsibilities delegated, if so, what authority accompanies accountability?

Q5:

a. Do your HR Dept and Information Security professionals (IS) coordinate efforts to embed a cyber security culture that promotes openness and best efforts in tackle cyber threats?
b. If yes, how? If no, why not?

Q6:

a. If so, who defined their responsibilities and what are the indicators that the board will support them in carrying out these responsibilities?

b. If not, how come you have the cyber security portfolio in your role of _____? I.e.: What is it in the organisational understanding that puts cyber security in your area rather somewhere else?

Q7:

a. if yes – how?

b. If no – what in the budget relates to cyber security, and in what way?

Appendix F: Phase 2. Themes gained from interviews

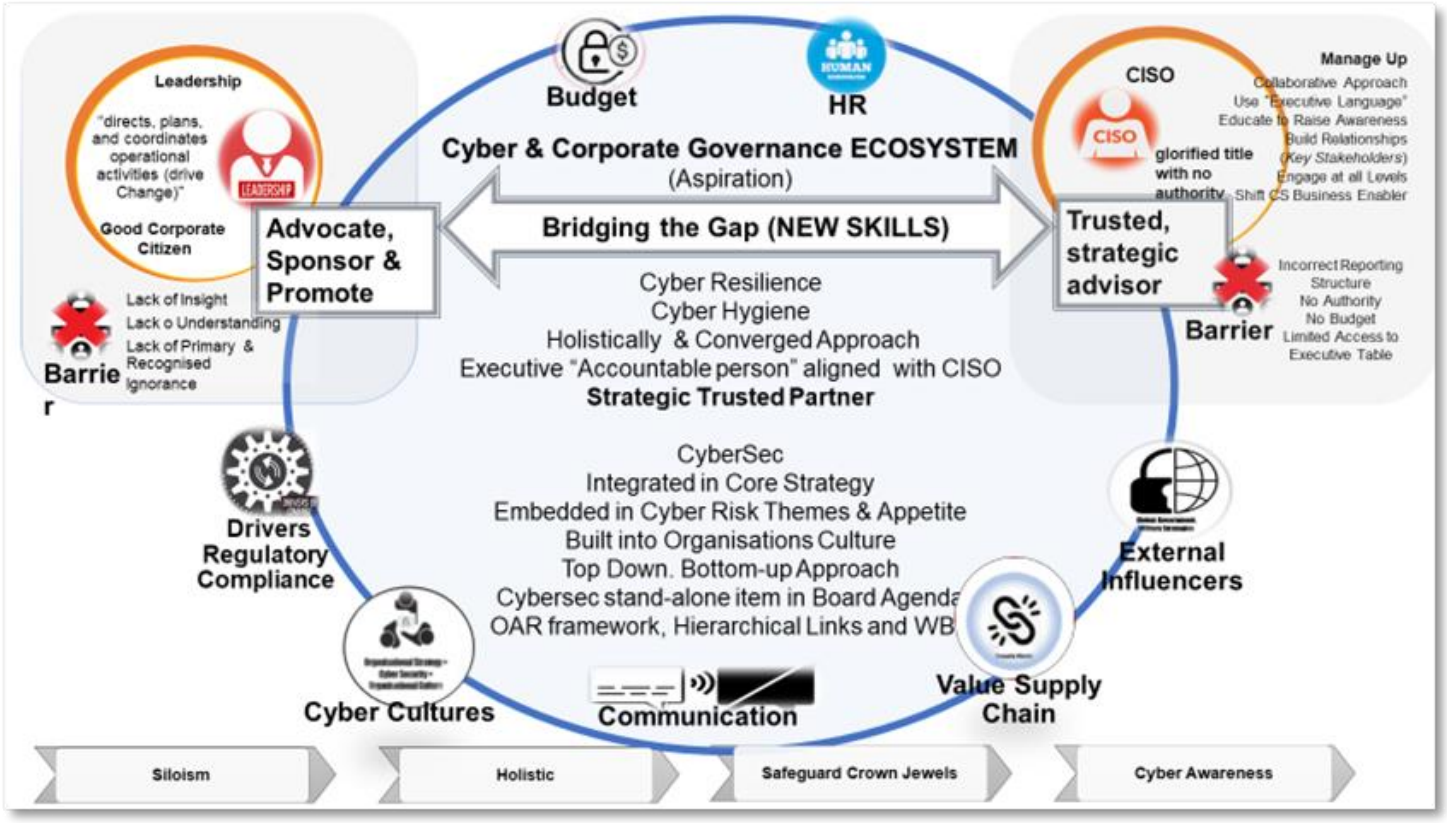

Figure A. 7.Themes gained from semi-structured interviews

Appendix G: Phase 2. Method: Analytical coding

Figure A. 8. Screenshot of a word cloud displaying dominant themes arising in early stages of analysis

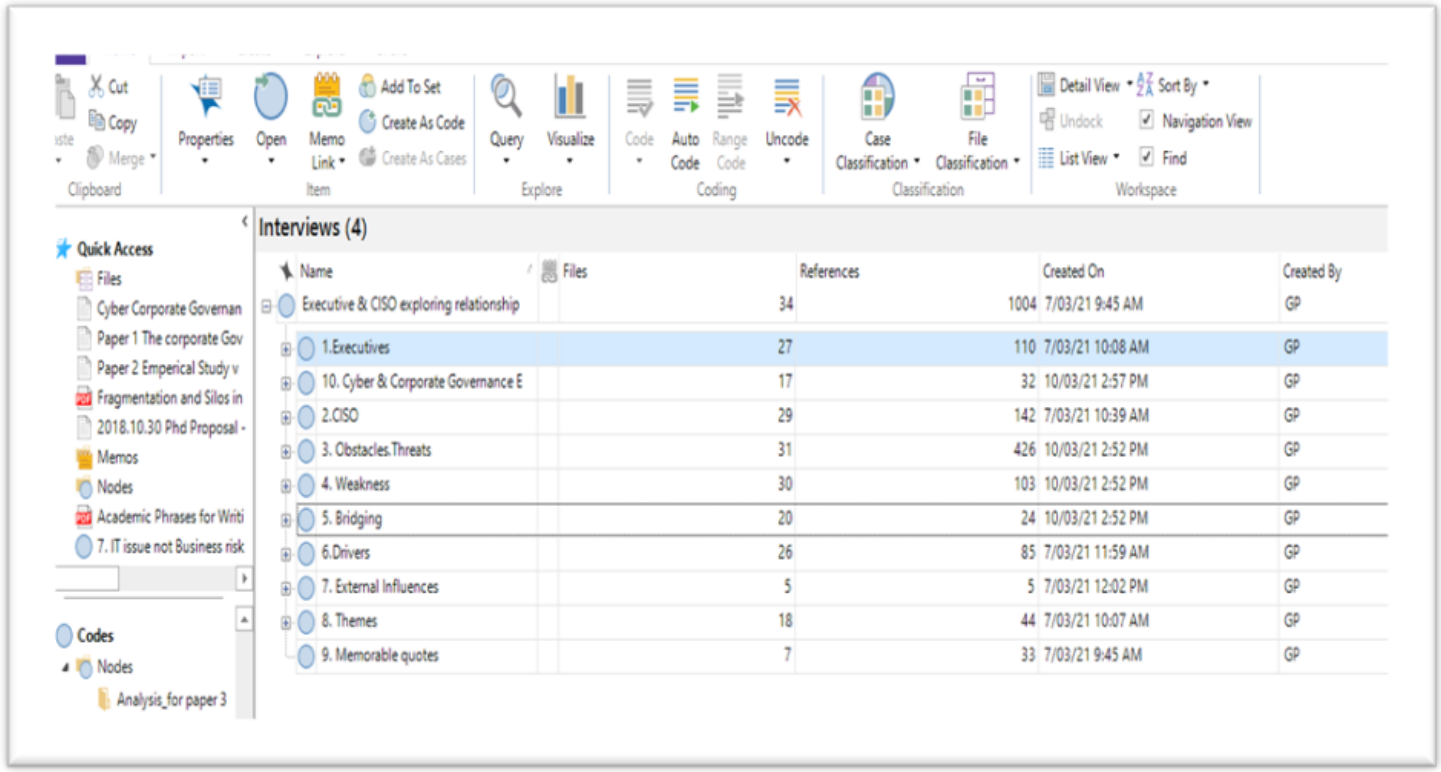

Figure A. 9. Screenshot of first qualitative coding of themes

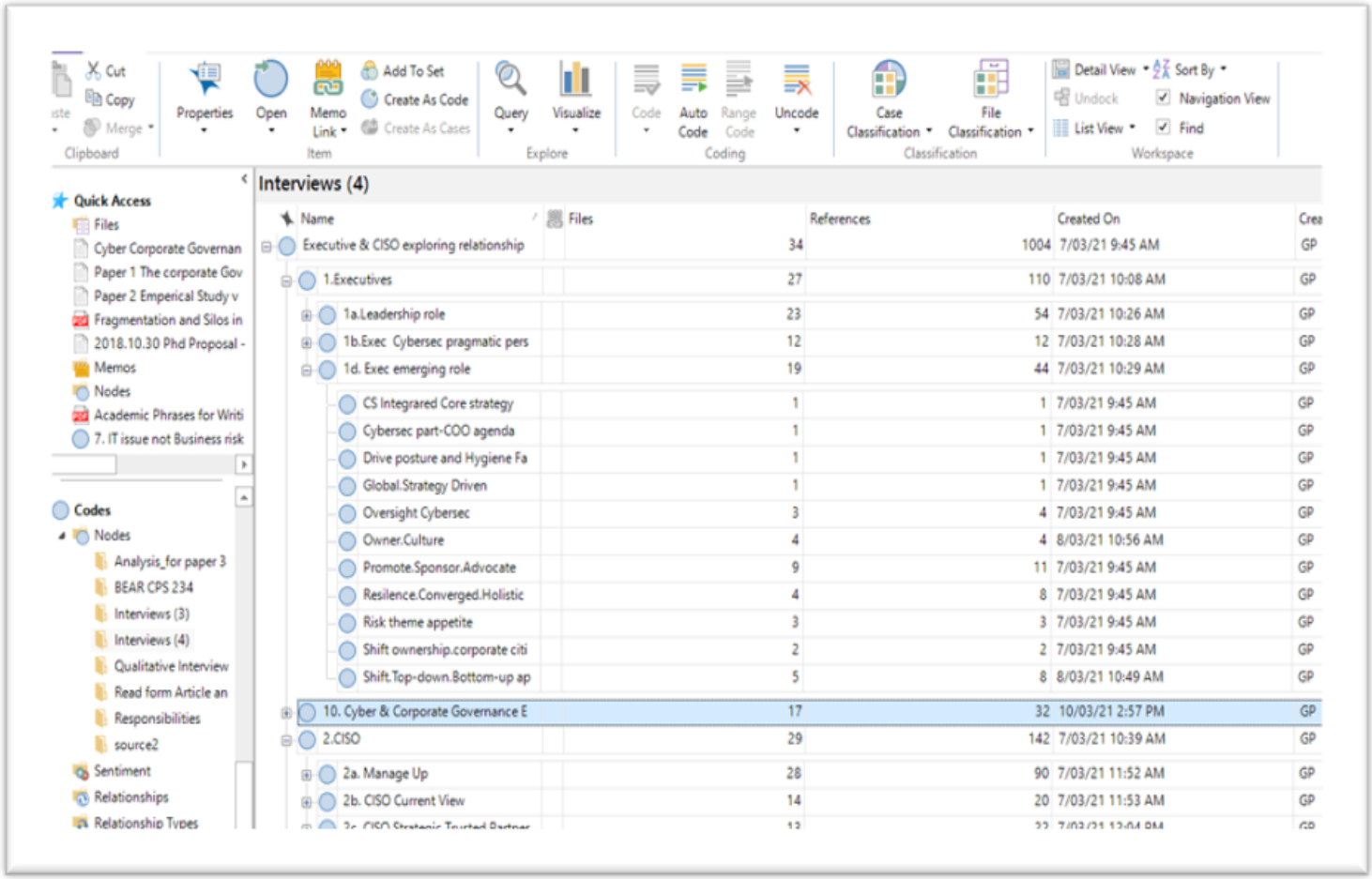

Figure A. 10. Screenshot of second pass identifying key themes

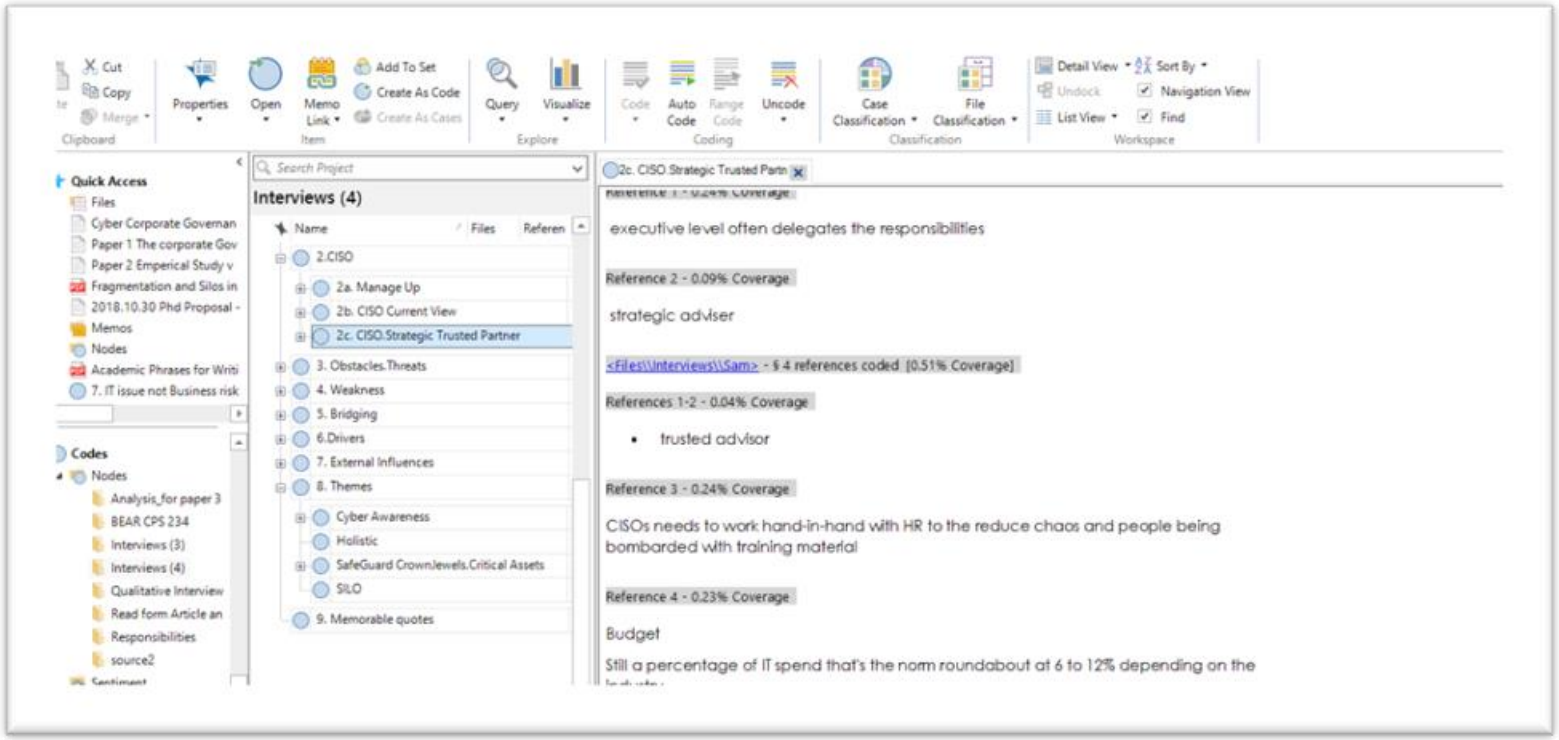

Figure A. 11. Screenshot of code contents with reference source example

Appendix H: Phase 2. Focused scoping review

Table A. 4 – Result by journal and ABDC rating

Author	Year	Journal	Field of Research	ABDC Rati	Result
Hambrick, DC	2007	*Academy of Management Review*	Management	A*	Executive
Kankanhalli, A., Teo, HH., Tan, BCY and Wei, KK	2003	*International Journal of Information Management*	Information Systems	A*	Executive
Lewicki, RJ., McAllister, DJ and Bies, RJ	1998	*Academy of Management Review*	Management	A*	Trust
Neely, BH., Lovelace, JB., Cowen, AP and Hiller, NJ	2020	*Journal of Management*	Management	A*	Executive OAR
Shao, Z	2019	*International Journal of Information Management*	Information Systems	A*	OAR
Wang, G., Holmes, RM., Oh, IS and Zhu, W	2016	*PERSONNEL PSYCHOLOGY*	Management	A*	Executive OAR
Hambrick, DC., Humphrey, SE and Gupta, A	2015	*Strategic Management Journal*	Management	A*	Executive
Heracleous, L & DeVoge, S	1998	*Long Range Planning*	Management	A	Executive
Narain Singh, A., Gupta, MP and Ojha, A	2014	*Journal of Enterprise Information Management*	Information Systems	A	Cyber Security
Poindexter, W	2019	*MIT Sloan*	Management	A	Cyber Security
Yap, C., Soh, C and Raman, K	1992	*Omega*	Management	A	Cyber Security
Zacharias, NA., Six, B., Schiereck, D and Stock, RM	2015	*Journal of Business Research*	Marketing/Tourism/Logistics	A	OAR
Lankton, N., Price, JB and Karim, M	2021	*Journal of Information Systems*	Information Systems	A	Executive OAR
Chen, WH, Kang, M and Butler, B	2019	*Management Decision*	Management	A	Executive OAR
Bakari, JK, Tarimo, CN., Yngström, L., Magnusson, C and Kowalski, S	2007	*Computers & Security*	Information Systems	A	Cyber Security
Phillips, R., Freeman, RE and Wicks, AC	2003	*Business Ethics Quarterly*	Management	A	Stakeholder Theory
Freeman, RE., Phillips, R and Sisodia, R	2018	*Business and Society*	Management	A	Stakeholder Theory
Karanja, E	2017	*Information & Computer Security*	Information Systems	B	CISO OAR
von Solms, R & Von Solms, B	2006	*Computers & Security*	Information Systems	A	Executive OAR
Von Solms, B & Von Solms, R	2018	*Information and Computer Security*	Information Systems	B	Executive OAR
Daud, M., Rasiah, R., George, M., Asirvatham, D and Thangiah, G	2018	*International Journal of Business and Society*	Accounting, Auditing and Accountability	C	Executive OAR

Karanja, E & Rosso, MA	2017	*Journal of International Technology and Information Management*	Information Systems	C	CISO OAR
Johnson, AM	2009	*Journal of Information Privacy and Security*	Information Systems	C	Executive Business and Security
Kappers, WM & Harrell, N	2020	*Journal of Applied Business and Economics*	Economics	C	CISO OAR

Appendix I: Phase 3. Resource (narrow) rigour ranking of cited references.

Search results identified only six peer-reviewed journals that used all three keywords combination that is “cyber security”, “information security”, “corporate governance” and “ecosystem” or “environment”. Further analysis found nine results using the terms “cyber security" and “corporate governance", and six using “information security” and “corporate governance”, while only six applied the terms “corporate governance” and “ecosystem”. The remaining five search results identified only one of these terms.

Table A. 5 – Summary result on group search using keywords and phrases

Result on group search using keywords and phrases		
Keywords	**Count**	**Percentage**
cyber security	*2*	*6.7%*
corporate governance	*3*	*10%*
cyber security; corporate governance	*9*	*30%*
corporate governance; ecosystem	*2*	*3.3%*
cyber security; environment	*2*	*6.7%*
cyber security; corporate governance; ecosystem	*1*	*6.7%*
cyber security; corporate governance; environment	*2*	*6.7%*
information security; corporate governance; environment	*3*	*10%*
information security; corporate governance	*6*	*20%*
	30	*100*

Table A. 6 – Results on group search using key phrases and keywords

We identify which disciplines’ journals published works on each of the targeted search terms and search terms combination in Table A. 7.

Field of research	Group search on key phrases and keywords					#	%
	Cyber security	Information Security	Corporate Governance	Ecosystem	Environme		
Accounting, Auditing and Accountability			✔			*1*	*3*
	✔		✔	✔		*1*	*3*
Applied Economics			✔	✔		*1*	*3*
Banking, Finance, and Investment			✔			*1*	*3*
Business and Management			✔			*1*	*3*
			✔	✔		*1*	*3*
	✔		✔			*3*	*10*
Information Systems	✔				✔	*1*	*3*
		✔	✔			*6*	*20*
	✔		✔			*5*	*17*
		✔	✔		✔	*3*	*10*
	✔					*1*	*3*
	✔		✔		✔	*1*	*3*
LAW	✔					*1*	*3*
	✔		✔		✔	*1*	*3*
	✔				✔	*1*	*3*

Other Commerce, Management, Tourism and Services	✔		✔			*1*	*3*
No of Discrete Disciplines # 7						*30*	*100*

Table A. 7 – Results by field of research, Journal and ABCD rating

The findings for the additional refined literature review just described are explained and discussed in the Refining the question section of this paper.

Field of research	Journal	ABDC rating	#	%
Accounting, Auditing and Accountability	Copernican Journal of Finance and Accounting	C	1	3.3
	International Journal of Business and Society	C	1	3.3
Applied Economics	Journal of Economic Surveys	A	1	3.3
Banking, Finance, and Investment	Journal of Banking & Finance	C	1	3.3
Business and Management	Harvard Business Review	A	1	3.3
	MIT Sloan Management Review	A	2	6.7
	Technological Forecasting and Social Change	A	1	3.3
	Journal of Management and Governance	C	1	3.3
Information Systems	Decision Support Systems	A*	1	3.3
	Information and Organization	A*	1	3.3
	Journal of the Association for Information Systems	A*	1	3.3
	Computers and Security	A	6	20
	Journal of Information Systems	A	1	3.3
	Digital Policy, Regulation and Governance	B	2	6.7
	Information and Computer Security	B	2	6.7
	Information Systems Management	B	2	6.7
	Information Systems Security	C	1	3.3
LAW	Stanford Journal of International Law	A	1	3.3
	Cornell International Law Journal	B	1	3.3
Other Commerce, Management, Tourism and Services	Journal of International Affairs	A	2	6.7
			30	100

Table A. 8 – Keywords results by Author, year, journal, field by research and ABCD rating

Author	Year	Journal	Field of Research	ABDC Rating	Result
Maynard, SB., Tan, T., Ahmad, A and Ruighaver, T	2018	Journal of the Association for Information Systems	Information Systems	A*	Information Security, Corporate Governance, Environment
Nambisan, S	2018	Information and Organization	Information Systems	A*	Cyber security
Pang, M-S	2014	Decision Support Systems	Information Systems	A*	Cyber security, Corporate Governance
Hepfer, M & Powell, TC	2020	MIT Sloan Management Review	Business and Management	A	Cyber security, Corporate Governance
Manita, R., Elommal, N., Baudier., P and Hikkerova, L	2020	Technological Forecasting and Social Change	Business and Management	A	Cyber security, Corporate Governance
Mihr, A	2014	Journal of International Affairs	Other Commerce, Management, Tourism and Services	A	Cyber security, Corporate Governance
Moore, JF	1993	Harvard Business Review	Business and Management	A	Corporate Governance, Ecosystem
Rattray, G., Gijsbers, K., Tikk, E., Purdy, A., Mulvenon, J and Carr, J	2011	Journal of International Affairs	Other Commerce, Management, Tourism and Services	A	Cyber security, Environment
Sadik, S., Ahmed, M., Sikos, LF and Islam, AKMN	2020	Computers and Security	Information Systems	A	Cyber security, Environment
Shackelford, SJ & Craig, AN	2014	Stanford Journal of International Law	LAW	A	Cyber security
Vatiero, M	2017	Journal of Economic Surveys	Applied Economics	A	Corporate Governance, Ecosystem
Von Solms, B	2001	Computers and Security	Information Systems	A	Information Security, Corporate Governance

Von Solms, B	2006	Computers and Security	Information Systems	A	Information Security, Corporate Governance
Von Solms, B & Von Solms, R	2005	Computers and Security	Information Systems	A	Information Security, Corporate Governance
Von Solms, R & Von Solms, SH	2006	Computers and Security	Information Systems	A	Information Security, Corporate Governance
Von Solms, SH	2005	Computers and Security	Information Systems	A	Information Security, Corporate Governance
Weill, P & Ross, JW	2005	MIT Sloan Management Review	Business and Management	A	Cyber security, Corporate Governance
Wilkin, C & Chenhall, R	2020	The Journal of information systems	Information Systems	A	Cyber security, Corporate Governance
Da Veiga, A & Eloff, JHP	2007	Information Systems Management	Information Systems	B	Information Security, Corporate Governance, Environment
Fidler, B	2017	Digital Policy, Regulation and Governance	Information Systems	B	Cyber security, Corporate Governance
Kuerbis, B & Badiei, F	2017	Digital Policy, Regulation and Governance	Information Systems	B	Cyber security, Corporate Governance
Mishra, S	2015	Information and Computer Security	Information Systems	B	Information Security, Corporate Governance, Environment
Peng, S	2018	Cornell International Law Journal	LAW	B	Cyber security Corporate Governance, Environment
Turel, O, Liu, P & Bart, C	2017	Information Systems Management	Information Systems	B	Cyber security, Corporate Governance, Environment
Von Solms B & Von Solms RS	2018	Information and Computer Security	Information Systems	B	Information Security, Corporate Governance
Ahmed, AAN	2019	Copernican Journal of Finance and Accounting	Accounting, Auditing and Accountability	C	Corporate Governance
Li, Z	2014	Journal of Banking & Finance	Banking, Finance, and Investment	C	Corporate Governance

Clapham, SE & Cooper, RW	2005	Journal of Management and Governance	Business and Management	C	Corporate Governance
Holzinger, A	2000	Information Systems Security	Information Systems	C	Cyber security, Corporate Governance
Daud, M., Rasiah, R., George, M., Asirvatham, D and Thangiah, G	2018	International Journal of Business and Society	Accounting, Auditing and Accountability	C	Cyber security, Corporate Governance, Ecosystem
Note: Journals listed in the Financial Times (FT List) with ABDC ranking of A					

Appendix J: Phase 3. Method: Analytical coding

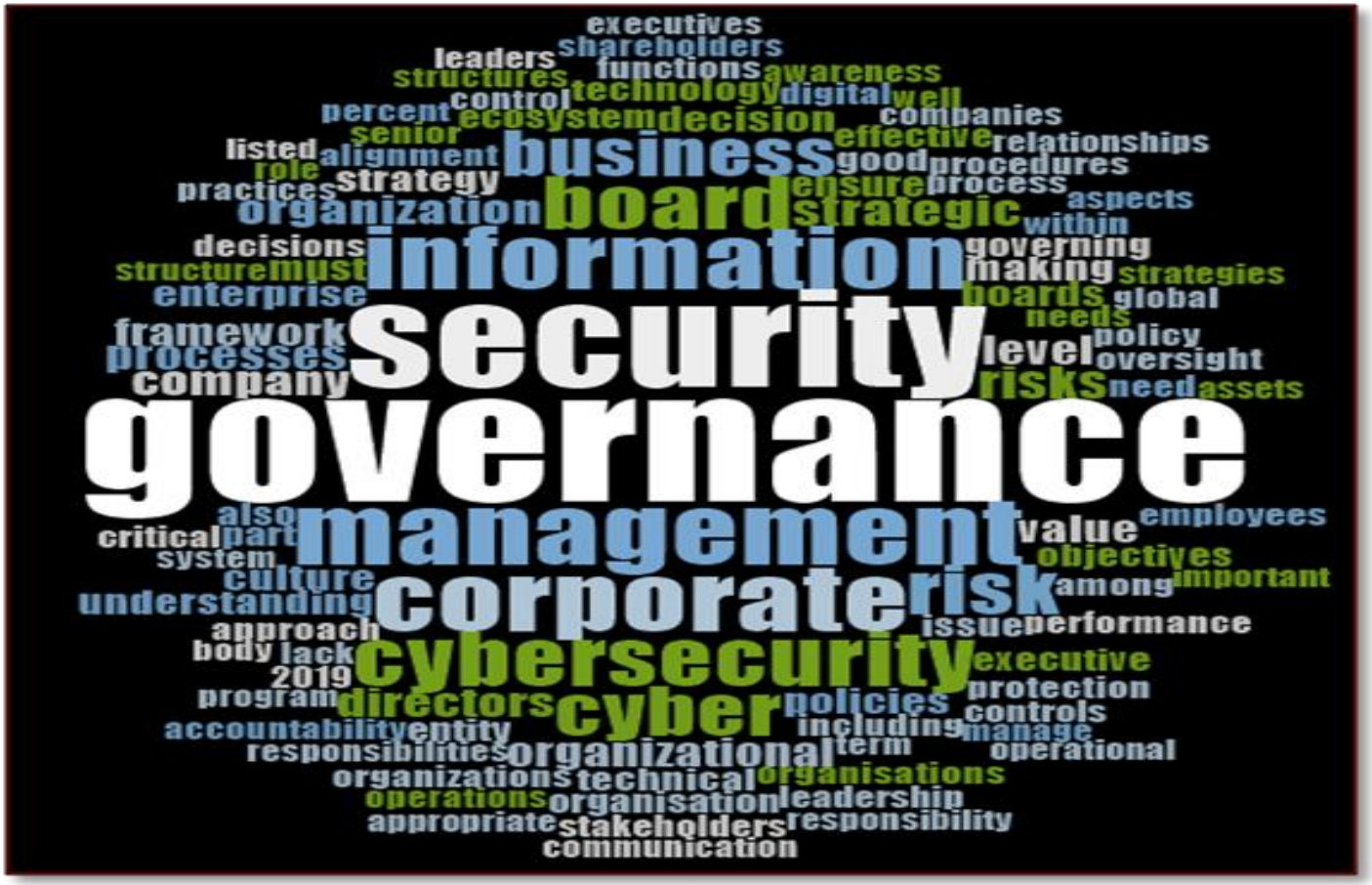

Figure A. 12. Screenshot of a word cloud displaying dominant themes arising in early stages of analysis

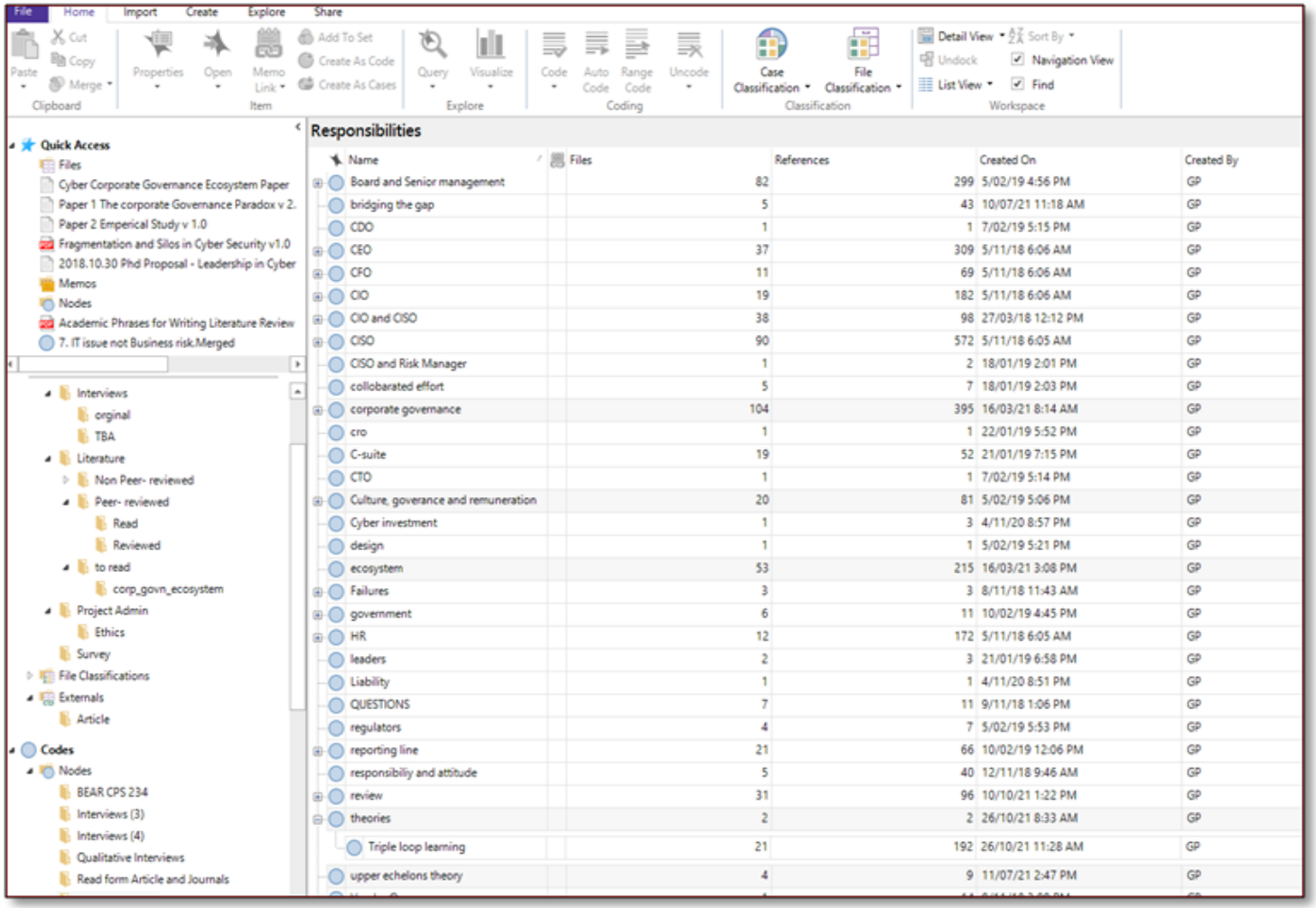

Figure A. 13. Screenshot of first qualitative coding of themes

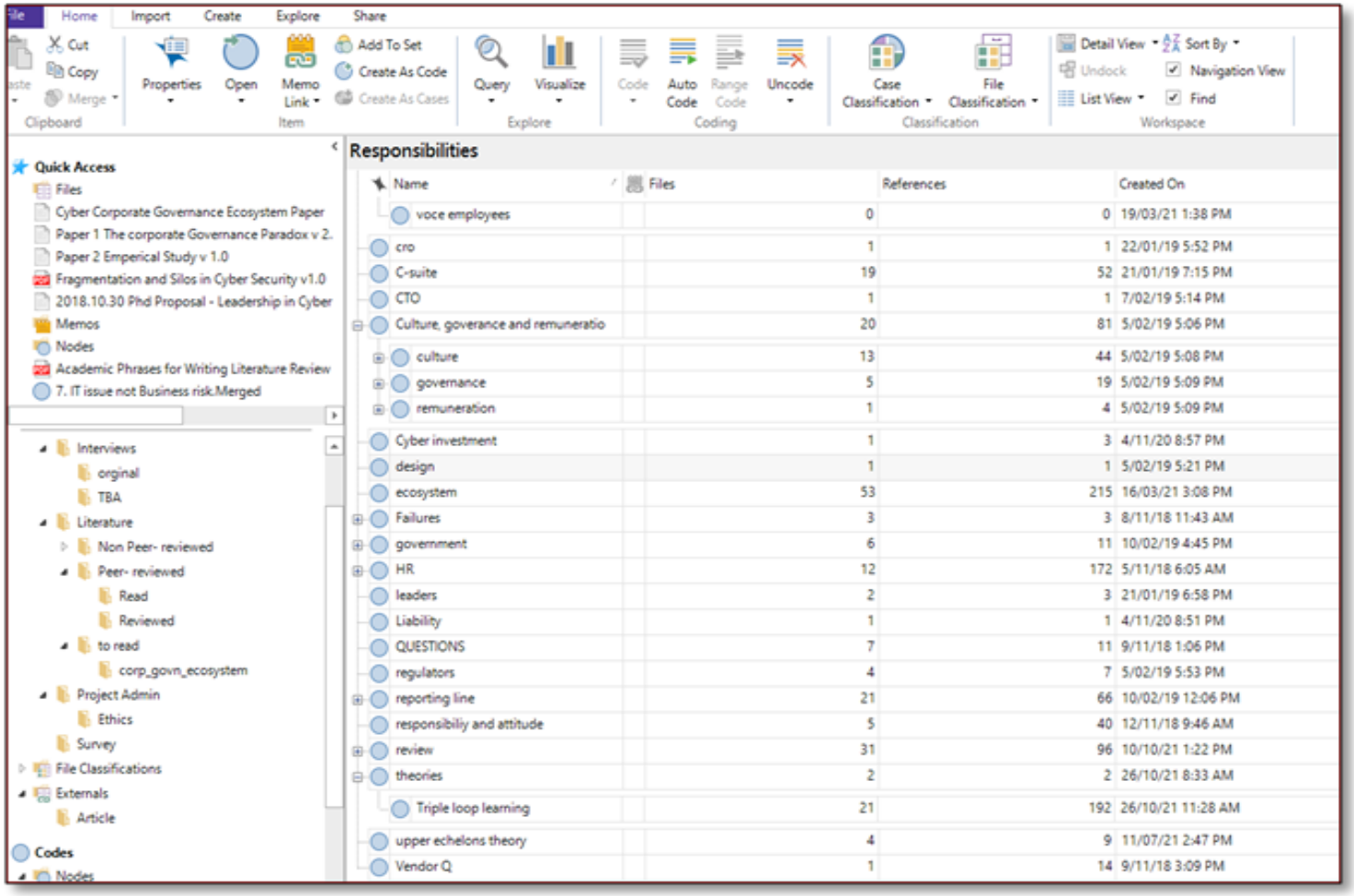

Figure A. 14. Screenshot of second pass identifying key themes

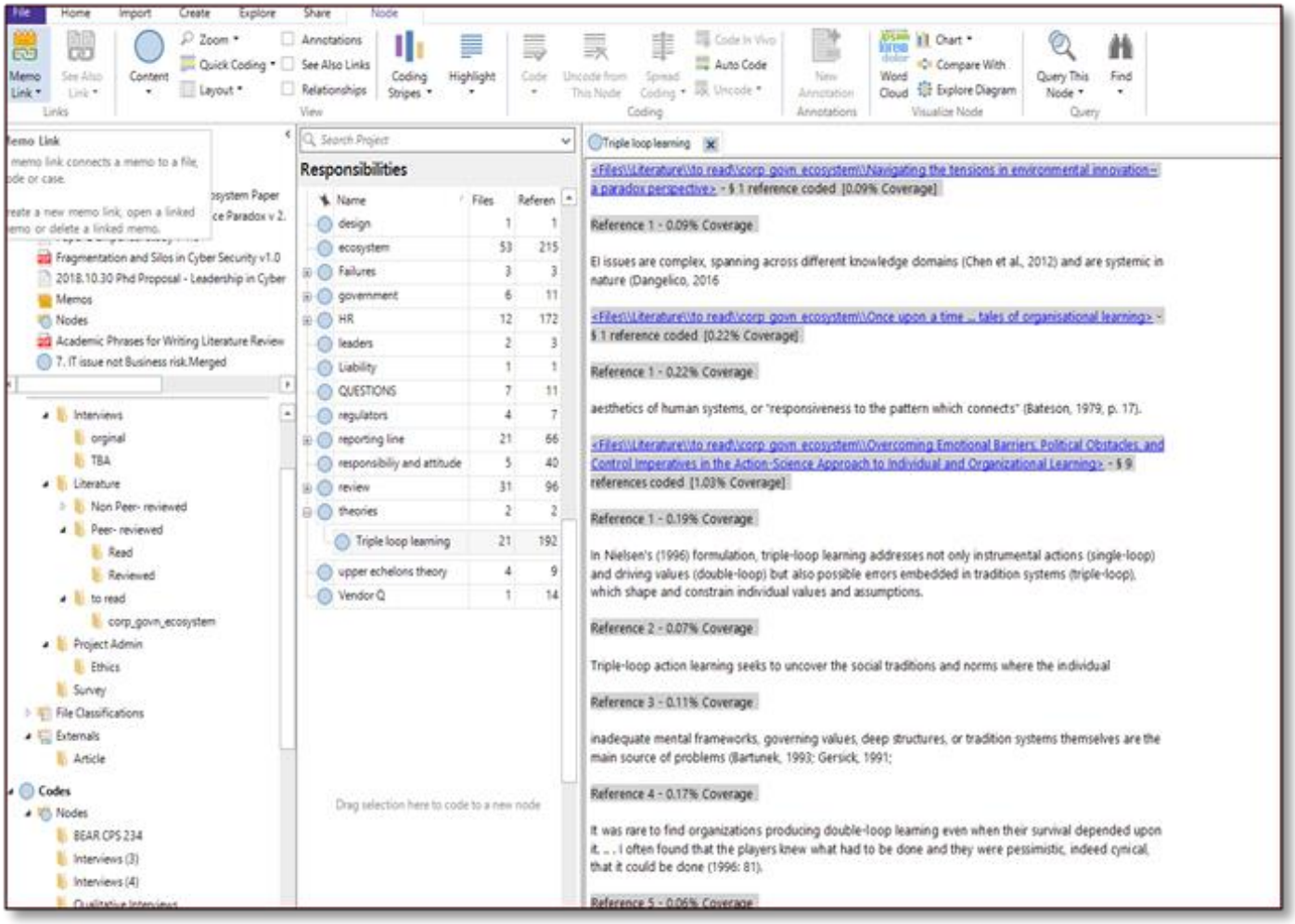

Figure A. 15. Screenshot of code contents with reference source example

Table A. 9 - Results by Field of Research and by Journal

Field of research	Journal	ABDC Rating	Count	Percentage
Accounting, Auditing and Accountability	International Journal of Business and Society	C		4%
	Journal of Applied Business ar Economics	C		4%
Information systems	Computers & Security	A		8%
	Information & Computer Security	B		4%
	Information and Computer Security	B		4%
	International Journal of Information Management	A*		8%
	Journal of Enterprise Information Management	A		4%
	Journal of Information Privacy and Security	C		4%
	Journal of Information Systems	A		4%
	Journal of International Technology and Information Management	C		4%
Management	Academy of Management Review	A*		8%
	Business and Society	A		4%
	Business Ethics Quarterly	A		4%
	Journal of Management	A*		4%
	Long Range Planning	A		4%
	Management Decision	A		4%
	MIT Sloan	A		4%
	Omega	A		4%
	Personal Psychology	A*		4%
	Strategic Management Journa	A*		4%
Marketing/Tourism/Logistics	Journal of Business Research	A		4%
			24	100%

Table A. 10 – Results by Field of Research and Key Phares and Keywords

Field of Research	Group Search on Key Phares and Keywords									Count	Percentage
	CISO OAR	Cyber Security	Executive	Executive	Executive OAR	Executive Business & Security	OAR	Stakeholder Theory	Trust		
Accounting, Auditing and Accountability					v					1	4%
Economics	✔									1	4%
Information Systems	✔	✔		✔	✔	✔	✔			10	42%
Management		✔	✔	✔	✔			✔	✔	11	46%
Marketing/Tourism/Logistics							✔			1	4%
No of Discrete Disciplines # 5	3	4	1	3	6	1	2	2	1	24	100%

Table A. 11 – Results by Key Phrases and Keywords

Result on group search using keywords and phrases	Count	Percentage
CISO OAR	3	12.5%
Cyber Security	4	16.7%
Executive	1	4.2%
Executive	3	12.5%
Executive OAR	7	29.2%
OAR	2	8.3%
Stakeholder Theory	2	8.3%
Trust	1	4.2%
Executive Business and Security	1	4.2%
Grand Total	24	100%

Appendix K: Abbreviations and acronyms

Table A. 12 – Acronyms

Acronym	Explanation
A3C	Australian Cyber Collaboration Centre
ACS	Australian Computer Society
ACSC	Australian Cyber Security Centre
ADF	Australian Defence Force
ADI	Authorised Deposit-Taking Institutions
AISA	Australian Information Security Association
APRA	Australian Prudential Regulation Authority
ASD	Australian Signals Directorate
ASIC	Australian Securities and Investments Commission
AustCyber	Australian Cyber Security Growth Network
B2U	Business-to-you
BEAR	Banking Executive Accountability Regime
CCCS	Canadian Centre for Cyber Security- Government
CDO	Chief Data Officer
CEH	Certified Ethical Hacker
CEO	Chief Executive Officer
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CGI	Computer-Generated Imagery Inc
CHRO	Chief Human Resource Officer
CIA	Confidentiality, integrity, and availability
CIA	Confidentiality, integrity, and availability

CIO	Chief Information Officer
CISO	Chief Information Security Officer
CLO	Chief Legal Officer
CMO	Chief Marketing Officer
COBIT	Control Objectives for Information and Related Technologies
COO	Chief Operating Officer
CPS 234	Consolidating prudential standards
CSO	Chief Security Officer
CSRC	Computer Security Resource Center
CSX	Cybersecurity Fundamentals
Digital Health	Australia Digital Health Centre, Australian Government
DST	Defence Science and Technology Group
FAR	Financial Accountability Regime
FPA	Financial Planning Association of Australia
GAP	Global Access Partners
GDP	Gross domestic product
GDPR	General Data Protection Regulation
HR	Human Resources
HREC	Human Research Ethics Committee
HRM	Human resource management
ICAEW	Institute of Chartered Accountants in England and Wales
ICT	Information and communications technology
IP	Intellectual property
IS	Information Systems

ISACA	Information Systems Audit and Control Association
$(ISC)^2$	International Information System Security Certification Consortium
ISO	International Organization for Standardization
IT	Information Technology
JBI	Joanna Briggs Institute
JCSC	Joint Cyber Security Centres
MBA	Master of Business Administration
NDB	Australian Government's Notifiable Data Breach
NICE	National Initiative Education
NIST	National Institute of Standards and Technology
NSW	New South Wales
OAIC	Office of the Australian Information Commissioner
OCA	Open Cybersecurity Alliance
PII	Personally Identifiable Information
RISCS	Research Institute in Sociotechnical Cyber Security
ROI	Return on Investment
ROI	Return on investment
SANS	SysAdmin, Audit, Network, and Security Institute
SAP	Systems Applications and Products in Data Processing
SMB	Small Medium Business
SOX	*Sarbanes-Oxley Act 2002*
STEM	Academic disciplines of science, technology, engineering, and mathematics
TAFE	Technical and Further Education
TAT	The Australian Tribute

TOLA	*Telecommunications and Other Legislation Amendment Act 2018*
WHS	Workplace health and safety

Table A. 13 – Glossary of terms

Term	Definition
Big 4	Refers to the four major Accounting consulting firms (Deloitte, EY, KPMG, PwC)
C-level or C-suite	A widely used term to describe a cluster of a corporation's most important senior executives. The letter C stand, for "chief" e.g., Chief Executive Officer (CEO), Chief Operating Officer (COO), and Chief Information Officer (CIO). Each of these individuals are in charge of particular area or department within the business (Bloomenthal 2021).
COVID-19	A highly contagious respiratory disease caused by the SARS-CoV-2 coronavirus. (NIH 2019)
Cyber defence	Cyber hygiene (maintenance and security) plus cyber resilience (Cyber security and business continuity)
Cyber hygiene	The process of implementing and maintaining cyber security best practices to protect and keep the organisation safe online from cyber-attacks (RSI SECURITY 2019; Tunggal 2020). Cyber hygiene procedures and processes: • secure configurations for all devices; • vulnerability assessment and remediation; • use of administrative privileges; • applying patches or software updates • aimed at maintaining the health of organisation. (Maennel, Mases & Maennel 2018)
Cyber resilience	The ability to continuously deliver mission-critical system capabilities and outcome despite adverse cyber events (Björck, Henkel, Stirna & Zdravkovic 2015).
Cybersec	Cyber security
The Executive	CEO and Board
infosec	information security
MBB	Three major management consulting firms (McKinsey, BCG, and Bain (MBB)
OAR	Ownership. Accountability and Responsibility
Regulatory Compliance	A means of ensuring the organisation is following the rules for its industry (Absolute 2019). Covers legislation, regulations, standards, guidelines, and frameworks which is endorsed and supported by advocates.
Siloism	Siloism in organisation. Siloed, isolated, barriers, turfism and cultural tribes. Organisational silos – "putting the 'parts' before the 'whole'" (Waal, Weaver, Day, & Heijden 2019, p. 3). Psychological boundaries (silo-mentality) creating compartmentalization, segregation, and differentiation between different parts of an organization. Inhibits cross-boundary collaboration and cooperation and organizational learning. Forestall a unified vision that awards organisational success and sustainability (Waal et al. 2019, p. 2).