Organisational Cyber Resilience: Management Perspectives

Saba Bagheri
University of Tasmania, Australia
seyedehsaba.bagheri@utas.edu.au

Gail Ridley
University of Tasmania, Australia

Belinda Williams
University of Tasmania, Australia

Abstract

As cyberthreats pose strategic risk, both IT and business management awareness are critical for effective organisational decision making. Many cyber system failures arise from organisational, and not technical issues. This study investigates senior manager awareness of organisational cyber resilience, using case study method. The Cyber Resilience Matrix is used as a theoretical framework to communicate the multifaceted meaning of cyber resilience. This study examines whether the multilayered nature of cyber resilience is understood by both managerial levels to include the periods before and after cyber incidents. As the higher education sector faces complex cyber challenges, research data were gathered from two Australian universities. Analysis found the two management groups differed in their resilience approach. The authors posit that principles-based cyber policies contribute to an organisational view of cyber resilience. The engineering resilience approach, accompanied by a non-bureaucratic organisational structure, was preferred by IT managers. Business managers favoured an ecological approach with a vertical organisational structure. Both managerial groups emphasised the period before cyber crisis when compared to after cyber incidents. This research contributes to the limited theoretical development in the field and attempts to shift the focus from cyber security to cyber resilience.

Keywords: Organisational cyber resilience, universities, senior IT managers, business managers, cyberthreat.

1 Introduction

While organisations depend on cyber activities (Ahmad et al., 2015; Cavelty, 2007), the cyber environment is frequented by cyber criminals (Conklin & Kohnke, 2018) and attempted intrusion from unfriendly nations (ABC News, 2020). Cyberthreats are now universal and affect all organisations. Although the most common approach to combat cyber threat is to use cyber security solutions (Vugrin & Turgeon, 2013), cyber security procedures are inadequate to deal with information security crises (Tisdale, 2016; Bagheri, 2020). To better prepare organisations for cyber threats, cyber resilience must be used in combination with cyber security (Trim et al., 2009).

Cyber resilience is the capacity of a cyber-system to perform effectively, regardless of the hazards (Vugrin & Turgeon, 2013). In contrast, cyber security is usually defined by the number of procedures that attempt to protect systems from different types of cyberthreats. In complex organisational environments, cyber solutions need to go beyond cyber security and

incorporate resilience (Colombo, 2020; Stouffer et al., 2011; Bagheri, 2020). The many approaches to achieve cyber resilience (Roege et al., 2017) reveal that cyber resilience is multi-disciplinary, and extends beyond technical issues to include behavioural and organisational aspects (Bernabe & Skarmeta, 2019; Sabev, 2020; Tisdale, 2016).

Scholarly research into cyber resilience has emphasised technical and operational aspects. Relatively few studies have considered the organisational elements of cyber resilience (Bagheri & Ridley, 2017; Sepúlveda-Estay et al., 2020). As cyber issues threaten business objectives, management awareness of organisational cyber resilience is essential for appropriate decision making (Soomro et al., 2016; Bagheri, 2020). Cyber problems cannot be solved only by technical decision makers. Business managers should be also included, as well as IT managers (Orozco et al., 2015). Despite the important role of business managers in the cyber security decision making process, studies indicate that business managers do not demonstrate appropriate knowledge of cyber security and resilience, leading to conflict between organisational cyber goals and business objectives (Johnson, 2009; Tisdale, 2016). To deal with this problem, a common understanding of cyber security and resilience is needed among senior IT and business managers from different functional roles (Johnson, 2009). Although the importance of managerial awareness of cyber security is discussed by researchers (Moallem, 2020), the issue of shared understanding by managerial groups has received limited attention in the cyber resilience literature. This study aims to investigate senior IT and business managers' shared awareness of cyber resilience, with a focus on organisational factors. As both roles are key for effective decision making for cyber crisis, alignment of the perspective of the two managerial groups will strengthen organisational cyber resilience.

A subsidiary aim of this study is to examine if the multilayered meaning of cyber resilience is understood by both managerial levels to include the periods both before and after cyber incidents. This study also seeks to understand whether the vertical or horizontal organisational structure is favoured by these two managerial groups. A further secondary goal is to investigate whether engineering or ecological resilience thinking is preferable for organisational cyber resilience decision making, as each resilience approach is likely to lead to different strategic decisions being taken by managers.

For the purposes of this research, organisational factors refer to a range of features and characteristics of an organisation that influence the workplace, including organisational structure, policies, social relationships and communication, decision-making processes, employee knowledge and skills, cultural issues and other elements (Goodman & Haisley 2007). The current study focuses on organisational cyber resilience and excludes cyber security and technical aspects of cyber resilience development. The scope of this investigation is limited to cyber resilience in two large organisations with complex cyber environments. The extreme cyber challenges faced in the higher education sector led to the decision to conduct the investigation within two Australian universities.

This research is motivated by a lack of research into organisational aspects of cyber resilience, the acknowledged tension between senior IT and business managers in understanding the role of cyber resilience and, in particular, the potential impact of poor strategic decision making for cyber crisis on organisations (Johnson, 2009; White, 2009). It focuses on the key role of both IT and business managers in developing a cyber resilient organisation, rather than the singular focus of the senior IT managerial role. Consequently, this research seeks to contribute to

shifting the focus from cyber security to cyber resilience, as well as highlighting the multidisciplinary nature of cyber resilience by examining its organisational aspects.

The literature on organisational cyber resilience is reviewed in the second section of this paper, with a brief discussion on the different perspectives of senior IT and business managers. The study's methodology appears in the third section, followed by the results and discussion in the fourth and fifth sections, respectively. Finally, the conclusions are presented in the sixth section, with limitations and recommendations for future research.

2 A review of organisational cyber resilience

The limited number of scholarly publications on organisational cyber resilience demonstrates that academic research into organisational cyber resilience is still at an early stage (Björck et al., 2015).

The concepts of resilience and cyber resilience first need to be differentiated, as well as the distinction between cyber resilience and cyber security approaches.

Forms of resilience

As resilience refers to the capacity of systems and organisations to absorb changes during adverse situations (Annarelli et al., 2020; Segovia et al.,2020), it is a primary enabler to cope with, adapt to, and recover from disturbance (Béné et al., 2014; Hausken, 2020). Resilience in an organisational context is applied in two ways—*engineering* and *ecological*—each of which results in a different approach to deal with threats. Engineering resilience refers to stability and the fast recovery of an organisation or system to its original condition (Holling, 1996; Sikula et al., 2015). Ecological resilience implies an organisational ability to adjust to a new situation (Berkes et al., 2008; Noureddine, 2020) through change, and focuses on learning from the crisis (Bellini & Marrone, 2020; Sikula et al., 2015).

To the best of the authors' knowledge, no scholarly research has investigated whether engineering or ecological resilience thinking dominates cyber resilient organisations. As each resilience approach is likely to lead to different strategic decisions being taken by managers, the authors were motivated to identify the type of resilience thinking that is preferable for organisational cyber resilience decision making.

Cyber resilience versus cyber security

Cyber resilience is a new paradigm which emphasises the business capability of an organisation to survive a cyberthreat (Bei, 2019; Buchmann et al., 2020). It encompasses "anticipation, support, recovery and adaptation" (Yano et al., 2015, p. 2) in a changing environment (Linkov et al., 2013a). In contrast, cyber security is explained as a set of policies, strategies and programs to defend cyber systems (Craigen et al., 2014), and imposes rules to restrict data access and minimise information risk (Antikainen, 2014). While the ultimate goal of both *cyber security* and *cyber resilience* approaches is to protect organisations against cyberthreats, researchers believe that resiliency should be added to cyber security studies (Le & Hoang, 2017). Cyber resilience thinking assists organisations to prepare for, and develop the ability to recover from, cyber risks and hazards (Annarelli et al., 2020; Roege et al., 2017), and is the capacity of a cyber-system to perform effectively regardless of the hazards in the business environment (Vugrin & Turgeon, 2013). Therefore, a cyber-resilient system not only focuses on providing protection against cybercrimes, but also considers the threat response

before, during and after an incident (Roege et al. 2017). The breadth of response aligns with Linkov et al.'s (2013b) definition of cyber resilience that includes the planning, absorption, recovery and adaptation stages.

Organisational cyber resilience

This study is limited to the organisational aspects of cyber resilience because of the latter's multifaceted nature (Buchmann et al., 2020) and the limited research into those dimensions compared to the technical aspects. Among the few academic studies available on organisational cyber resilience, the Cyber Resilience Matrix includes organisational aspects of cyber resilience (Linkov et al., 2013b). The framework maps four organisational domains (i.e. physical, information, cognitive, social) from the Network Centric Warfare (NCW) (Alberts et al., 2000), to four stages of event management (i.e. plan/prepare, absorb, recover, adapt) in cyber resilience adapted from the National Academy of Sciences (NAS) (National Academy of Sciences, 2012). While the Matrix includes cyber resilience metrics to identify an organisation's capability to deal with cyber crises, it does not aim to identify the organisational factors that contribute to cyber resilience. More explanation about this matrix is provided in the next section.

Shapiro et al. (2016) of the World Economic Forum extended the Linkov et al. (2013b) framework by amalgamating it with the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity, which has since been updated. The Shapiro et al.'s framework is complex and includes a fifth event management stage, Detection with the authors acknowledging data collection limitations. It is also noted the framework was not designed to identify organisational factors for cyber resilience.

Other studies have identified factors for organisational cyber resilience in a fragmented way. For example, the Sarkar et al. (2013) conceptual model of the information systems resilience of Small- and Medium-sized Enterprises (SMEs) referred to business continuity and recovery planning, the leadership role, cultural issues, and external organisational elements. Although the 2013 study examined internal and external elements of cyber resilience and emphasised the decision-making process, it was limited to SMEs and did not consider the larger organisational context. Other studies have developed organisational evaluation tools and best practices for cyber resilience. To illustrate, Hult and Sivanesan (2014) proposed a cyber resilience checklist with questions for self-assessment, Ferdinand (2015) designed a knowledge-based cyber resilience structure, while Lykou et al. (2018) proposed cyber resilience best practices for smart airport systems. The evaluation tools and best practice approaches provided by these studies were designed to help organisations better understand their cyber resilience. However, it is important to note the aim of the tools was not to identify the organisational factors of cyber resilience.

Other researchers considered the recovery phase (e.g. Conklin & Shoemaker, 2017; Appiah et al., 2020) without examining the remaining cyber resilience event management stages of planning, adaptation and absorption (Linkov et al., 2013b). However, no frameworks were identified in these and other academic studies for examining the organisational factors of cyber resilience.

Other organisational cyber resilience studies from the limited literature include Gisladottir et al. (2016) who examined the selection of an appropriate number of rules for cyber resilience development. While their study focused on the absorption and recovery phases of resilience

with an emphasis on organisational regulations, less emphasis was given to other aspects of cyber resilience (e.g. post incident). Another study examined engineering resilience models and human behaviour to develop a framework that combined four resilience functions (anticipate, monitor, respond and learn) with three characteristics of behaviour (capability, opportunity and motivation) (van der Kleij & Leukfeldt, 2019). In a further publication that investigated cyber resilience development in financial corporations, researchers identified three main approaches to promote cyber resilience, namely: 1) cyber resilience enhancement as the cyber security future, 2) inclusion of cyber resilience into cyber security standards bodies, and 3) cyber resilience development through creating compliance tools (Dupont, 2019). While the last two studies contributed to a better understanding of non-technical aspects of cyber resilience, the managerial role did not receive attention in either.

A recent study by Kott and Linkov (2021) sought to measure cyber resilience, suggesting use of a measurement process utilised in material science and physics. The authors believed that additional criteria relevant to cyber systems should be developed, including repeatability, consistency and monotonicity. They recommended use of a large volume of data to increase the confidence level in measuring cyber resilience (Kott & Linkov, 2021). Again, the Kott and Linkov (2021) study neither considered any organisational aspect of cyber resilience nor any managerial aspects.

Annarelli et al. (2020) developed a Managerial Cyber Resilience Framework using six case study organisations. The proposed framework listed the managerial actions required in the (single) planning/ preparing phase of event management. Although the study interviewed several key informants from case studies to understand managerial actions, it did not investigate a senior managerial perspective on organisational cyber resilience. In another study, Loonam et al. (2020) developed a Cyber Security Strategy Framework (CSSF) to be used by managers for effective cyber resilience strategy development. The CSSF framework suggested that managers should focus on governance and transformational support (security culture). However, while the CSSF highlighted the important role of senior managers in cyber resilience development by proposing managerial strategies for adoption, it did not investigate their perspectives on organisational cyber resilience.

From the review above, it can be seen that while some non-technical aspects of cyber resilience appear in the scholarly literature, no structured framework of the organisational factors of cyber resilience was found. The frameworks, models, and studies of organisationally-oriented cyber resilience examined in the literature review are collated in Table 1, and categorised by their orientation.

Of the studies identified, the Cyber Resilience Matrix (Linkov et al., 2013b) was the most comprehensive in characterising the meaning of cyber resilience. The Cyber Resilience Matrix (hereafter referred to as the Matrix) (Linkov et al., 2013b) includes activities that occur b*efore* (i.e., planning) and *during*/*after* (i.e., absorption, recovery, and adaptation) cyber crisis across four cyber event management stages. Other researchers examined only one or two stages of event management for managing cyber crisis (e.g. Conklin & Shoemaker, 2017 and Roege et al., 2017). However, all stages of event management need to be considered. A cyber-resilient organisation not only focuses on the period before the cyber threat (planning stage of cyber security handling), but also on the threat response during and after (absorption, recovery, and adaptation) an incident (Roege et al., 2017). The Matrix is examined in more detail in the following section.

Framework/ study name	Major components	Author/ Year
Measuring Cyber Resilience	Discusses the importance of cyber resilience measurement through well-developed measurement process	(Kott & Linkov, 2021)
Managerial Cyber Resilience Framework	Managerial actions required in the planning/ preparing phase of event management.	(Annarelli et al., 2020)
Cyber Security Strategy Framework (CSSF)	Focuses on governance and transformational support (security culture)	(Loonam et al., 2020)
Cyber resilience in financial corporations	Three main approaches to promote cyber resilience	(Dupont, 2019)
Integrated model from Engineering Resilience & Human Behaviour	Combines four resilience functions (anticipate/ monitor/ respond/ learn) & three sources of behaviour (capability/ opportunity/ motivation)	(van der Kleij & Leukfeldt, 2019)
Cyber resilience best practices for smart airport systems	Three groups of best practices for technical/ organisational/ policies & standards	(Lykou et al., 2018)
Seven principles for cyber resilience	Seven principles to establish cyber resilience (classify/ risk/ rank/ design & deploy/ test/ recover/ evolve)	(Conklin & Shoemaker, 2017)
An algorithm for recovery and response activities	Framework of three main activities (standard maintenance activities/ supporting activities/ emergency response and recovery activities)	(Roege et al., 2017)
Cyber resilience and over & under regulation	Resilience is a function of the number of rules in an organisation	(Gisladottir et al., 2016)
A Framework for Assessing Cyber Resilience	Framework that combined Linkov et al. (2013b) and the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity.	(Shapiro et al., 2016)
Knowledge-Based Structure for Cyber Resilience	Five stages of cyber resilience: (Non-existent / Immature /Established /Reactive /Fully proactive & reactive cyber resilience)	(Ferdinand 2015)
Cyber Resilience Checklist	Checklist of nine cyber resilience items	(Hult & Sivanesan, 2014)
Cyber Resilience Matrix	Matrix that relates areas of disaster resilience (NCW) with steps of event management (NAS)	(Linkov et al., 2013b)
Information Systems (IS) Resilience Conceptual Framework	Consists of external & internal elements for IS resilience in SMEs	(Sarkar et al., 2013)

Table 1. Organisational cyber resilience frameworks and studies, arranged in year order

2.1 Cyber Resilience Matrix

The Matrix used NAS's stages of event management for cyber resilience in the horizontal axis, with NCW's four domains of an organisation or system in the vertical axis.

The four stages of cyber event management are:

- Plan/ Prepare: maintain service accessibility during disruptions;
- Absorb: operational availability;

- Recover: rebuild resource functionalities, and
- Adapt: learn from incidents, and update procedures where required (Feist, 2006; Hambleton et al., 2000; Linkov et al., 2013b).

The four organisational domains are:

- Physical: physical sources;
- Information: information relevant to the physical layer;
- Cognitive: decision-making procedures, and
- Social: organisational relationships (Linkov et al., 2013b).

Each cell of the Matrix includes metrics that aim to evaluate the system capability to manage a cyber crisis. The Matrix appears in Table 2, with example metrics to illustrate what each cell refers to.

The research on organisational cyber resilience is fragmented, with a limited theoretical foundation. In their review of the literature on organisational aspects of cyber resilience, Bagheri and Ridley (2017) found the matrix perspective was one of three approaches taken to examine the topic. While no scholarly framework of cyber resilience's organisational factors and strategies was identified by the authors, the Cyber Resilience Matrix (Linkov et al., 2013b) is more comprehensive than other frameworks, with the exception of the complex Shapiro et al.'s (2016) framework.

Linkov et al.'s (2013b) Matrix was refined by Shapiro et al. (2016), to assess industry and sector cyber resilience. That framework combined Linkov et al.'s (2013b) framework with the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity. Shapiro et al's (2016) refined framework was not used for this study due to its complexity. The authors discussed their difficulty of obtaining data to satisfy the framework's criteria in the framework. Also, the cyber resilience matrix Linkov et al's (2013b) is well established in the literature while the Shapiro et al's (2016) framework is complex and yet to be fully considered by the literature.

In an extensive review of resilience, Linkov and Trump (2019) referred to the "resilience matrix" in Chapter Six, and illustrated it in Chapter Eight. Another review of different approaches to measure the cyber resilience of autonomous agents discussed the Matrix as a qualitative approach (Ligo et al., 2021).

Linkov and associates' application of the Cyber Resilience Matrix to many diverse contexts was found in the literature. The following studies illustrate this range. In a literature review of how critical infrastructure resilience was modelled when encountering compounding or cascading threats, Wells et al. (2022) used the "Resilience Matrix" in their assessment. Linkov and co-authors used the Matrix to investigate the resilience of smart water systems (Marchese et al., 2019), community resilience assessment (Fox-Lent et al., 2015) and population displacement arising from disaster (Rand et al., 2019).

It can be seen that the literature on the Matrix is narrow, being largely derived from Linkov from the US Army Engineer Research and Development Center, and his associates.

In this study the multifaceted meaning of cyber resilience captured by Linkov et al. (2013b) will be used to analyse managers' understanding of organisational cyber resilience. The Matrix

will also provide the research with a theoretical guide in a new field that lacks research interconnections.

	Cyber Event Management Stages				
	Plan/prepare for		**Absorb**	**Recover from**	**Adapt to**
Organisational Domains	**Physical**	Maintain controls for cyber resources/create physical assets/evaluate systems interconnections	Use redundant services to continue operation/ reduce cyberthreats	Resolve any system problem/assess cyber risk/evaluate recovery time/change irrecoverable items	Evaluate the system's configuration/ allocate new assets
	Information	Classify information resources/ prepare documents for IT suppliers/store valuable information/identify internal or external relationships	Identify the sensors/transfer information to relevant parties	Store log data for databases/ recover after an incident	Keep records of time taken between the incident, recovery and post-recovery solution
	Cognitive	Plan for cyber incidents/understand business objectives/organise cyberwar gaming	Apply a protocol for decision-making/evaluate achievements/identify important resources/develop appropriate policies	Identify any breakdown points/ make decisions during recovery	Review management response for a better decision/ discover the reasons behind the cyber attack
	Social	Communicate with external parties/provide training programs/delegate services to particular employees/improve resilience communication among employees/foster a culture of cyber resilience	Identify & communicate with cyber resilience professionals	Follow cyber resilience guidelines/determine responsible parties for cyber resilience	Evaluate employees' response to cyber incidents/allocate human resources/remain up-to-date about cyber risks

Table 2. Cyber Resilience Matrix (Linkov et al., 2013b)

The next section briefly reviews the literature that examines differences between business and IT management groups.

2.2 Differences between IT managers and business managers

Previous research has investigated the importance of the senior managerial role for cyber resilience in organisations. Senior manager support is critical to developing cyber resilience (Bernard, 2007; McFadzean et al., 2007), as effective cyber resilience strategy starts at the top organisational level (Dutta & McCrohan, 2002). However, senior technical managers are not solely responsible for cyber resilience; business managers are also accountable (Selby, 2017). Strategic approaches to cyber security and resilience must consider broad organisational solutions in addition to the technical aspects (Chapman et al., 2018), as the socio-technical approach best fosters a security culture. The current research addresses a tension between the acknowledged criticality of engaging both technical and business managers in organisational cyber decision making, with a lack of academic research that examines the awareness of the topic by business managers.

A review of the literature on IT and business managers' perspectives of cyber resilience suggests that the two managerial groups have different views on the organisational factors that contribute to cyber resilience (Cobo et al., 2014; Fitzgerald, 2007; Rainer Jr et al., 2007). For example, in the IT-business alignment literature, business managers were found not to have a comprehensive understanding of IT issues (Bergeron et al., 2004; Luftman et al., 1999). If the perceptions of IT and business managers are visualised as a continuum, business managers are located at the business-focused end, unlike IT managers (Rainer Jr et al., 2007). As research on cyber security investment found business managers believed that allocating cyber security funds was not a business enabler, further discussions between business and IT managerial groups are required to align their knowledge and perspectives to benefit the organisation (Johnson, 2009). Teo and King (1997) argued that discrepant views between managers are rooted in their different positions and job responsibilities. Researchers have called for IT managers to help business managers enhance their understanding of IT issues (Al-Surmi et al., 2020; Armstrong & Sambamurthy, 1999; Wang et al., 2012), aiming for better IT resource allocation and strategic cyber security decision making within organisations (Tallon, 2014).

Divergent perspectives on cyber resilience by IT and business managers pose a risk for organisational decision-making, including insufficient provision of funding and other resources. A lack of awareness of organisational cyber resilience among IT and business managers may also lead to inconsistent decisions or inadequate actions to combat cyber crisis. However, the issue has received relatively little attention in the research literature. This study will investigate the organisational contributors of cyber resilience, and compare IT and business managers' awareness of organisational cyber resilience.

3 Methodology

This research used a case study methodology approach in two Australian universities to investigate senior management awareness of cyber resilience. The case study method provides an organisational setting that allows detailed knowledge to be gathered about a topic (Berg, 2004; Merriam, 2009). Large and complex business environments are favoured by cyber attackers because of sensitive personal and financial information stored in their databases. Universities are large organisations with challenging cyber environments that are exposed to numerous cyber attacks and significant cyber incidents. When university staff and students connect personal devices to network resources (Wagstaff & Sottile, 2015), they create an open environment for data exchange. Consequently, universities are challenged to establish full

control over information flows and cyber issues. As the authors reside in Australia, they have been exposed to media reports of cyber infiltration in Australian universities (Borys, 2019). For instance, the top ranked Australian National University (Quacquarelli Symonds, 2018) experienced a serious cyberattack in 2017, and still worked to reduce the impact of that attack a year later (Austin, 2018). Australian universities have been described as weak when dealing with cyber problems and cyber security, and as a result, they have worked to enhance their cyber resilience strategies to deal with cyber crisis (Austin, 2018). The cyber challenges faced by Australian universities motivated the authors to investigate cyber remediation strategies in university case studies to identify the organisational contributors to cyber resilience development in large complex organisations.

Differences between Australian universities prompted the researchers to broaden the scope of the study beyond a single case study to two case studies. Diversities in the universities chosen were designed to allow the researcher to observe any common patterns while also providing contrasting data for the study. Unique access to the two universities and their willingness to participate in the current research project also influenced the researcher to select the particular universities as case study settings.

With just 43 universities in Australia, only limited information is provided in Table 3 to maintain the universities' anonymity.

	Location	**Total students**	**Total staff members**	**Number of campuses**
Case Study 1 (C1U)	Australian State A	Less than 40000	Less than 5000	Less than 5
Case Study 2 (C2U)	Australian State B	More than 40000	More than 5000	More than 5

Table 3. Broad characteristics of the two university case studies

A semi-structured interview technique was employed for data collection after obtaining ethics approval. A pilot study assessed the appropriateness of the developed interview questions after review by three researchers and revision of the questions. Nine open-ended questions were posed during the interviews, with the specific questions being tailored for each managerial group based around common themes (Table 4). The questions were designed to examine cyber resilience decision making, important cyber policies, required cyber skills and other organisational contributors to cyber resilience from the management perspective:

Interview question themes
Decision making process during a cyber crisis
Policies and strategic actions for cyber resilience
Important knowledge and skills for cyber resilience
Organisational contributors to cyber resilience
Suggestions to improve cyber resilience

Table 4. Main interview question themes

Seventeen senior managers from the two Australian universities were interviewed; nine were IT managers and eight came from business. Appendix A provides demographic information about the interviewees. The interviews were conducted between September 2017 and August

2018, and ranged from 15 to 55 minutes each. They were audio recorded and transcribed before analysis using the automated textual analysis software program, Leximancer. Leximancer identifies word synonyms and frequency in text passages as concepts, before visualising their interconnectedness in themes. The software allows patterns to be observed that may not be apparent from manual coding, while the validity and reliability of Leximancer analysis has been evaluated and confirmed (Smith & Humphreys, 2006).

Analysis was carried out at the theme level, where each theme represented an organisational factor of cyber resilience. Two analyses were undertaken:

1) In the first analysis, the organisational cyber resilience awareness of senior IT and business managers was compared after merging data from the two case studies. To allow comparison, the identified organisational factors for cyber resilience were categorised into the Matrix (Linkov et al., 2013b) cells to determine how organisational cyber resilience was understood by participant groups, as is explained next.

To classify each cyber resilience organisational factor identified into cell(s) of the Matrix, the Matrix metrics were first investigated to determine the meaning that best matched each factor. To illustrate, one organisational factor identified from analysis referred to *the importance of cyber resilience training programs for employees*. This factor aligned with the metric, *provide staff members with cyber resilience training programs*, located at the intersection of the ***plan/prepare*** *column and* ***the social*** *row* of the Matrix (Linkov et al., 2013b). Consequently, this factor was allocated to *the plan/prepare for social* cell. In some cases, a single organisational factor could be matched to more than one metric of the Matrix. In these instances, the organisational factor of cyber resilience was allocated to all relevant cells. In contrast, where organisational factors of cyber resilience could not be matched to any of the cell metrics, the items were ignored.

2) The second analysis compared the IT manager and the business manager data for each case study. This analysis aimed to identify similarities and differences between the IT and business manager groups within each case study.

For a deeper analysis, the cyber security/resilience policies from both case studies were also investigated to identify any potential differences between the universities. The contents of the policies were first reviewed and then compared with the organisational factors and strategies for cyber resilience identified from the primary data. Cyber security policies in both case studies helped the researcher to understand their directives for cyber security management.

4 Results

The results of the merged cases data analysis for senior IT and business managers are reported in the next four sections. Findings from each management group are also categorised into the Cyber Resilience Matrix cells.

4.1 Merged cases data- Senior IT manager analysis

The primary concept themes obtained from analysis of the merged cases interview text for senior IT managers appear in the Leximancer concept map in Figure 1 below with the same themes ranked on the right. Based on Leximancer hit counts, the most highly ranked themes are 'Tools', 'Communication', 'External' and 'Policies'.

Transcripts associated with each theme presented in Figure 1 were examined for their meaning. The organisational factors of cyber resilience identified from these themes, with

example participant transcript passages, appear in Table 5. Each identified organisational factor was codified in the column at the right, where *IT* refers to IT senior managers and F indicates an organisational factor.

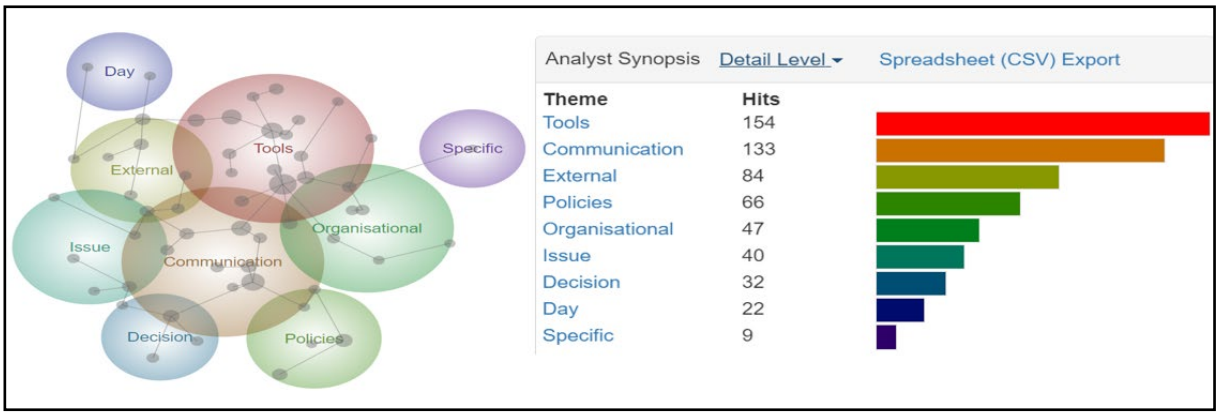

Figure 1. Concept map and ranked themes for organisational factors of cyber resilience—IT senior managers (merged case data)

Organisational factors identified in Table 5 were then categorised into the relevant Matrix cells. Corresponding codes for the organisational factors were noted in a bracket beside the relevant Matrix metric, as seen in Table 6. Cells without a metric matched to an organisational factor or strategy are shaded.

Theme	Example IT senior managers' transcript excerpt	Organisational factor	Code
Tools	I think there needs to be training [for cyber resilience]. Every organisation should have some mandatory training, I'm actually talking about how to stay safe (Interviewee 14).	*Importance of cyber resilience training programs for employees*	ITF1
	We try to be proactive, we do take a lot of steps [actions] from the ethical hacking that goes on in here. We guide them [ethical hackers] to watch systems that we think have the most exposure to the external world, like financial systems, customer information accounts, passwords. We should think from the perspective of hackers (Interviewee 6).	*Enhance proactivity (e.g. ethical hacking)*	ITF2
Commu-nication	We tend to delegate a lot of decision-making and trying to do things down to team members [*sic*]. The reason we do that is if something does happen, we don't have to wait an hour, or two hours or three hours for the CIO [Chief Information Officer] to make a decision about what needs to be done … So, we tend to expect … the frontline staff or the employees … [will] make decisions and act quickly (Interviewee 17).	*Make decisions during recovery with delegating decisions to skilled employees*	ITF3
	[After cyber crisis] I like to recover the core systems as quickly as possible. That would be where I would put my efforts. (Interviewee 8).	*Fast recovery of core systems (after cyber crisis)*	ITF4
External	IT can go often to recover systems, but we need to know who is responsible for cyber resilience. We also need to receive advice from other organisations. So, we need to know who are the key stakeholders of other organisations (Interviewee 7).	*Enhance cyber resilience through communication with both responsible parties and other external organisations*	ITF5
	Good technical products … appropriate tools … good knowledge of markets of the vendors and … understanding of	*a) Use modern cyber security tools and*	ITF6

	… technical tools are the most important [organisational factors] for cyber resilience. (Interviewee 15).	*technologies to support organisational systems*	
External	IT can go often to recover systems, but we need to know who is responsible for cyber resilience. We also need to receive advice from other organisations. So, we need to know who are the key stakeholders of other organisations (Interviewee 7).	*Enhance cyber resilience through communication with both responsible parties and other external organisations*	ITF5
	Good technical products … appropriate tools … good knowledge of markets of the vendors and … understanding of … technical tools are the most important [organisational factors] for cyber resilience. (Interviewee 15).	*a) Use modern cyber security tools and technologies to support organisational systems*	ITF6
Policies	I've seen an example [of a complicated cyber security policy] when I was in my last job at …University of … … I'm sure no one read them…! You need to have short and simple policies… I think they should be easy to read, sliced and as short as possible, so it communicates the business objective (Interviewee 9).	*Aim for 'simplified' cyber security policies to understand business objectives*	ITF7
	We need to have policies as part of our plan for cyberthreats. But I reckon as few [cyber security] policies as possible. If … [they] get too long, I wouldn't read them… And I know my guys [staff members] wouldn't read those policies. They would never have time to read it … they would never remember them (Interviewee 13).	*b) Have a limited number of cyber security policies for cyberthreat planning*	ITF8

Table 5. Organisational factors of cyber resilience—IT senior managers (merged case data).
Note: An explanation of the process of developing the organisational factors and their link to the Matrix appears in Section 3 (Methodology).

	Plan/prepare for	Absorb	Recover from	Adapt to
Physical	Create physical assets [**ITF6**]			
Information			Recover after an incident [**ITF4**]	
Cognitive	Plan for cyber incidents [**ITF8**]/understand business objectives [**ITF7**]/organise cyberwar gaming [**ITF2**]		Make decisions during recovery [**ITF3**]	
Social	Communicate with external parties [**ITF5**]/provide staff members with cyber resilience training [**ITF1**]/delegate services to particular employees [**ITF3**]	Identify & communicate with cyber resilience professionals [**ITF5**]	Determine responsible parties for cyber resilience [**ITF5**]	

Table 6. Organisational factors of cyber resilience located into the Cyber Resilience Matrix—Senior IT managers (merged case data)

Analysis results for the combined cases business manager data are reported next.

4.2 Merged cases data—business managers

Eight themes were identified in an analysis of the business managers' data. The Leximancer concept map labelled with themes is displayed in Figure 2, while the ranked themes appear at the right.

As this study seeks to identify the main differences between the grouped senior IT and business managers' views of organisational cyber resilience, only the highest ranked themes from the concept map were selected (see the right of Figure 2). Again, the theme ranks were identified based on hit numbers, so that the theme with the highest hit count indicates the most important theme in the concept map. As seen in Figure 2, 'Awareness', 'Team', 'Manager' and 'Organisation' were the most highly ranked themes. To understand the meaning of each theme, associated transcripts were reviewed. The organisational factors of cyber resilience identified from these themes, with example participant transcript passages, appear in Table 7. Each organisational factor was codified in the column at the right, where B refers to business managers and F indicates an organisational factor of cyber resilience (e.g. BF1 refers to the first organisational factor identified by business managers).

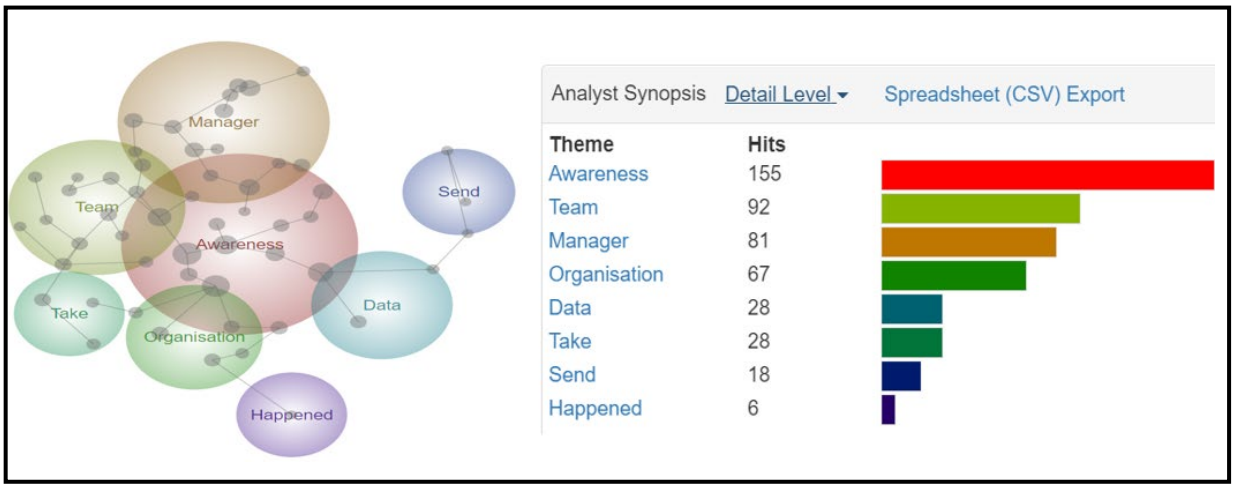

Figure 2. Concept map with ranked themes for organisational factors of cyber resilience—business managers (merged case data)

Ranked Theme	Example business manager transcript excerpts	Organisational factor	Code
Awareness	To me, one issue is making sure that people are aware or should be aware [of cyber resilience]. So, it's always around, trying to make sure that more people are aware of these things [cyber resilience issues] (Interviewee 3).	*Raise cyber resilience awareness among employees*	BF1
	They [IT teams] can help unpack technically what that resolves, but effectively, there is an element of responsibility that sits [at]… Executive levels. So, if you take my role [as a business manager], if I didn't take that issue [cyber resilience] seriously, there will be no resourcing for that … It always requires an understanding and communication [between IT department and business managers] for better [cyber] security (Interviewee 10).	*While cyber security experts are needed in the IT department, also take advice from, & communicate with, business managers*	BF2
Team	If you've got an organisation where employees are not satisfied with their jobs, cyber resilience is probably going to be one of the last issues on their mind… (Interviewee 2). [I]f you have unhappy employees, they could potentially be the ones that impact [negatively] on cyber resilience (Interviewee 1).	*Employee satisfaction*	BF3

Manager	Senior managers need to make decisions [during cyber crisis] and others should follow their advice. So, there should be a structured decision making system when a senior manager is responsible for taking decisions (Interviewee 5). So, yes, it is senior managers through the [cyber security] crisis that make the decisions, … they [senior managers] should take final decisions (Interviewee 11).	*Having a structured decision making system with the senior managers as decision makers*	BF4
	I suppose that IT is where they stop hackers get[ting] in. It is IT employees where they've got control over the systems to stop [it] happening. For example, in my team, we've got four system accountants. If they see … strange issues, they report it [to IT department]. So, we've got IT that is looking after cyber security, say all the information … we need to just keep an eye. So, if something looks strange, we need to report it straight away (Interviewee 12).	*Communicate with appropriate cyber security experts*	BF5
Organisation	Another issue is that you need to close down any future [cyber security] risk … So, you do things in a way that sometimes might be slower than you want, but you do it in a way that you don't have further compromised systems. So, you reduce any further exposure that you might have to data breaches (Interviewee 4).	*Mitigate potential cyber security risk*	BF6

Table 7. Organisational factors of cyber resilience—business managers (merged case data)

The organisational factors identified in Table 7 were next categorised into the most appropriate cells of the Matrix. A corresponding code for each organisational factor was recorded in a bracket beside the relevant Matrix metric, as shown in Table 8.

Plan/prepare for		**Absorb**	**Recover from**	**Adapt to**
Physical				
Information	Plan for sensitive information [**BF6**]			
Cognitive		Apply a protocol for decision-making [**BF4**]		
Social	Provide staff members with cyber resilience training programs [**BF1**]/improve resilience communication [**BF2**]	Identify and communicate with cyber resilience professionals [**BF5**]		

Table 8. Organisational factors of cyber resilience positioned in Cyber Resilience Matrix—business managers (merged cases data)

The next two sections present results for each senior management role after separate analysis of the interview data for each case study.

4.3 Case Study One— Senior IT versus business managers

The cyber resilience organisational factors identified from the C1U senior business manager data were similar to those for the same group from the merged data (see Table 7). However, analysis of the senior IT manager data from C1U revealed an additional cyber resilience organisational factor when compared with the same group for the merged data. The newly identified factor is presented in Table 9, with an example interview passage.

Example senior IT manager transcript excerpt—C1U	**Additional Organisational Factor**
We want to invest [by] … looking at our tool sets, and again I suppose when you are saying about unknown threats, it's really ensuring we keep our tool sets up-to-date and revisit and throw them out and get some new ones in (Interviewee 7).	*Importance of technical tools*

Table 9. Additional identified organisational factor—IT managers, C1U

The results of data analysis for the senior IT and business managers from C2U are presented next.

4.4 Case Study Two— IT senior versus business managers

Analysis of the senior IT and business manager data at C2U found no difference between the business managers' results and those from the merged case data for the same group (see Table 7). A difference was found in the results for the C2U senior IT managers, as three new organisational factors emerged. These organisational factors are seen in Table 10 with example transcript passages.

Example Senior IT managers' transcript excerpts—C2U	**Additional organisational factor**
We are very targeted with our [cyber resilience] advice rather than keeping it generic. [For example] … we use stories that we tell to employees and they remember stories, and that has an impact on their behaviour. We provide them with practical advice, specific and particular experience. (Interviewee 16).	*Raise awareness among employees through practical advice*
I think it needs more communication between these two groups [senior managers and employees] to understand what happens, and why, and how to address it (Interviewee 13).	*Communicate with employees*
I think employees follow cyber security rules more when a cyber crisis happens. For example, if the Cryptolocker virus was going around, a lot of employees were more aware and more careful because of the few incidents that happened. So, if they are concerned about a crisis, they might be more careful about security (Interviewee 15).	*Create concern about cyber security breaches among employees*

Table 10. Additional identified organisational factors—Senior IT managers, Case Study Two

The two analyses to investigate senior IT and business managers' awareness of organisational cyber resilience found differences between these managerial groups. The Discussion section elaborates on the differences found.

5 Discussion

5.1 Merged case data— Senior IT versus business managers

The results of the senior business manager merged case analysis indicated that this group favoured a more vertical and bureaucratic organisational structure (see BF4 in Table 7) compared to the senior IT managers (see ITF3 in Table 5). Senior business managers placed less emphasis on operational staff for decision making for cyber crisis. However, senior IT managers emphasised the employee role in decision-making, favouring a more horizontal organisational structure. Past research has suggested that when senior managers seek advice from IT employees for fast decision-making during cyber crisis, their organisations benefit (Davis et al., 2016; Hult & Sivanesan, 2014). The divergent results obtained for the senior IT and business manager groups from the merged case data signals that senior IT managers were

more aware of the key role of IT employees in cyber resilience development, a finding that is consistent with previous research (Linkov et al., 2013b).

Senior business managers had a more non-technical view of organisational cyber resilience when compared to senior IT managers. IT managers typically have specialist IT technical training. While senior IT managers emphasised use of modern cyber security tools and technologies to support organisational systems (see ITF6 in Table 5), the technological aspects of cyber resilience did not receive attention from senior business managers (see Table 7). These differences derive from the groups' different responsibilities, as business management roles cover more organisational and non-technological issues. Senior IT managers also emphasised the important role of employee training (see ITF1 in Table 5) in addition to the technological development of cyber resilience (see ITF6 in Table 5). Carias et al. (2018) concluded that investment in the technical elements of cyber security alone contributes to short-term cyber resilience improvement, while cyber resilience training enhances long-term cyber resilience development. That senior IT managers in the current study valued both technological tools and cyber security training for organisations suggests that they were aware of the importance of long-term cyber resilience development, as well as the needs for short-term cyber resilience improvement. However, greater communication between the two managerial groups may bring the business management perspective closer to the technical view (Rainer Jr et al. 2007).

While senior IT managers argued for fast recovery after cyber crisis (see ITF4 from Table 5) the current study also found that senior business managers favoured cyber security risk mitigation without emphasising fast recovery (see BF6 from Table 7). Reflection upon these two perspectives, suggests that business managers adopt an ecological approach to cyber resilience by placing less importance on the length of the recovery period after cyber crisis (see Table 7). This new finding contributes to the body of knowledge by suggesting how the response of both management groups differed. Our finding offers a pathway to strengthen cyber resilience, by combining both approaches.

As discussed earlier, minimising recovery time is important in engineering resilience, while fast recovery has less emphasis in ecological resilience thinking. Instead, ecological resilience stresses learning from adverse events (Sikula et al., 2015). The engineering resilience thinking of senior IT managers is important as an organisation must quickly recover from an adverse event. Otherwise, the organisation may not survive in a complex and competitive business environment, in which provision of services to customers, and continuing the core business function are fundamental. However, attending to fast recovery while ignoring learning from past incidents may result in the same adverse events in the future. Learning from past cyber incidents is aligned with the ecological resilience view of business managers. Differences in the ecological and engineering resilience perspectives of senior business and IT managers may contribute to the lack of shared cyber resilience understanding identified.

Cyber resilience is a business-IT issue (Sharma, 2015; Tisdale, 2016), one that requires both perspectives. Consequently, utilising both the IT manager (engineering resilience) and the business manager (ecological resilience) perspectives for cyber resilience development is likely to advantage organisations. This finding from the study is reinforced by Sikula et al.'s (2015) recommendation that in ideal resilience systems, both ecological end engineering resilience approaches need consideration. It is possible that enabling both approaches to organisational resilience to inform responses to cyber attack may contribute to an organisation being more adaptive.

As seen in Table 6 and Table 8, the cross-sectional cell, **plan/prepare x social**, had the highest number of organisational factors identified by both senior IT and business managers. This finding suggests that planning for the social domain was the most important cyber resilience issue for both management groups. Factors highlighted in the social domain include communication with external parties, improving resilience communication, providing staff members with cyber resilience training and delegating services to particular employees. While senior IT managers gave similar attention to the cross-sectional cell, **plan/prepare x cognitive** (see Table 6), the business managers' results did not emphasise the cognitive domain with its decision-making function (see Table 8). This finding suggests that while planning for both the social and cognitive domains was paramount for senior IT managers, decision-making (cognitive layer) procedures for cyber resilience improvement were unimportant for business managers. This distinction between the two management groups is likely to be associated with their different views on decision-making procedures during cyber crisis. Communicating with employees and delegating decisions when handling cyber security problems were practices favoured more by senior IT managers than business managers (see Table 5).

Both managerial groups were found to emphasise the *planning* phase when compared to the other event management stages of cyber resilience. However, as the definition of cyber resilience includes the period both *before and after* cyber crisis (Dewar, 2017; Yano et al., 2015), underestimating the contribution of the other phases may restrict cyber resilience development in organisations (Hausken, 2020). Limiting the attention paid to the non-planning phases reduces the capability of organisations to respond to cyber threats because the activities for absorption, recovery and adaptation stages occur after a cyber security incident is identified. Further, establishing cyber resilience policies takes place both before and after cyber crisis, since these policies are updated across the post-incident stage.

Analysis of the senior business managers' data revealed that the group ignored the period after cyber crisis, as the *recovery* and *adaptation* stages (see Table 6 and Table 8) received no attention. However, senior IT managers did emphasise the recovery stage of the Matrix for cyber resilience, but not the adaptation stage. These findings reinforce the dominance of engineering resilience thinking by senior IT managers, as noted in earlier reporting of the results. Fast "recovery" of systems after a cyber crisis is emphasised in the engineering approach as a strategy of cyber resilience (Sikula et al., 2015).

Another difference between the two management groups was observed in the *physical* layer of the Matrix. An example of factors located in the physical layer is maintaining controls for cyber physical resources and assets (e.g. network structure and system components) (Table 2). While senior business managers gave no attention to the physical domain (Table 8), senior IT managers did (Table 6). Although the focus of this research is on organisational cyber resilience, the physical aspects of cyber resilience should not be neglected. All four organisational domains need attention from managers (Linkov et al., 2013b).

The new findings identified in this study regarding the two senior manager groups' focus and/or inattention on particular event stages and organisational domains of the Matrix presented above, contribute to the body of knowledge. The results of this research may help explain how the actions and viewpoints of senior IT and business managers differ and are similar, and point to strategies for bringing the two perspectives together to strengthen organisational cyber resilience.

Despite the Matrix's aim to help organisations assess their system capacity for cyber incidents, this research found that some organisational and behavioural factors that influence cyber resilience were omitted from the Matrix. Employee satisfaction and organisational structure were identified as cyber resilience organisational factors from the interviewee data. However, these factors were not matched to any of the cell metrics. The omissions suggest that the Matrix is incomplete and may benefit from extension to include additional non-technological aspects of cyber resilience. The results from analysis of the separate case data are discussed next.

5.2 Separate case data— Senior IT versus business managers

As stated in the Results section, no difference was found between the senior business manager results within each separate case study, and those of the merged data for the same position. However, differences were found through analysis of the senior IT managers' results, where C1U IT managers followed a more technical approach when compared with the same group at C2U (Table 9). C2U senior IT managers adopted broader organisational perspectives on cyber resilience (Table 10). To better understand the difference between these two groups, the cyber security/resilience policies from both case studies were investigated. The interview transcripts were also reviewed to explain these differences.

C2U had conducted awareness campaigns with staff and students about cyber security, while similar approaches were not discussed in the C1U interviews. The C2U campaign produced and displayed posters describing recent cyber-attacks to increase cyber security awareness. One C2U interviewee explained: 'We have … posters for cyber security. It's all about security issues … *(to)* reinforce … *(to)* employees to *(help them)* understand these issues. I think this can develop a common sense of what is security. *(W)*e use stories that we tell to employees and they remember stories … that … *(have)* an impact on their behaviour' (Interviewee 17). The campaign appeared to shape senior IT managers' thinking in C2U by focusing on the broader human and organisational aspects of cyber resilience, in addition to the technical issues.

Another issue that may help account for the differences found between the senior IT manager groups in the two case studies was that two senior IT managers at C2U held responsibility for less technical areas, such as assisting users during a cyber crisis and translating business needs to IT solutions. One senior IT manager from C2U explained: 'Most of my team is involved in security from a consultancy perspective, helping users with security problems, so when they feel threatened, we all … *(are)* the first respondents. We should help them to understand that their behaviours …*(pose)* the most risks, rather than their password being breached or anything like that.' (Interviewee 15). In contrast, the job descriptions of C1U senior IT managers did not convey a similar broad role. The broadened responsibilities seen in C2U appeared to enrich senior IT managers' understanding of the organisational, non-technical issues of cyber resilience.

Differences in the cyber security policies at each university were found from both the policy review and the interview transcript analysis. One of the senior IT managers at C2U stated: 'We have a high level … master policy here rather than too … *(many)* policies' (Interviewee 13). Another IT manager interviewee from C2U commented: 'I think we are focusing on security advice rather than policies. We achieve cyber security through advice and education rather than *(by)* creating policies' (Interviewee 16). C2U had fewer cyber security policies compared to C1U despite its larger size. The former university believed that more policies would not be beneficial. The cyber security policies at C2U were general and organisational cyber security guidelines more than technical policies. However, the cyber security policies at C1U were

detailed and technologically-based, in addition to being more numerous. C2U IT management believed that a limited number of high level, principles-based, cyber security policies made it easier for managers and users to remember important issues. Broader policies imply a principles-based approach, where organisational policies are developed using high-level guidelines. In a rules-based approach, detailed prescriptions are provided to stakeholders on how to behave (Burgemeestre et al., 2009).

6 Conclusion

This study sought to address the lack of scholarly research into organisational cyber resilience by investigating perceptions held by senior managers from large organisations. While major effort has been invested by previous scholars in developing organisational cyber security, this study sought to shift research focus from cyber security to cyber resilience, and emphasised the multidisciplinary nature of the latter. Limited prior related academic research has used an established cyber resilience framework to study organisational cyber resilience, contributing to restricted theoretical development in this young field.

This research used the multifaceted meaning of cyber resilience proposed by Linkov et al. (2013b) in which the periods both before and after the cyber crisis also require management. The research applied an accepted cyber resilience model, the Cyber Resilience Matrix (Linkov et al., 2013b), as a theoretical foundation to identify differences between IT and business managers' perspectives on organisational cyber resilience at two Australian university case studies. Seventeen senior IT and business managers were interviewed, along with analysis of each university's cyber security policies.

From analysis of the organisational factors identified in this study placed into the Cyber Resilience Matrix, this study found that the stage related to *before* cyber crisis (i.e. planning) received more attention when compared to the stages *after* cyber incidents (i.e. absorption, recovery and adaptation phases). Consistent with a definition of cyber resilience which covers before, during and after cyber security incidents (Linkov et al., 2013b), cyber-resilient organisations need to consider all three stages of cyber security to be able to handle cyber threats. This finding points to the value for senior IT and business managers in placing more emphasis on the during and after cyber security crisis stages to strengthen cyber resilience. From analysis, the authors recommend extending the Cyber Resilience Matrix (Linkov et al., 2013b) to include further behavioural and organisational elements (employee satisfaction and organisational structure), to reflect a more holistic view of organisational cyber resilience. The results highlight the value of having a limited number of principles-based cyber security policies covering both technical and organisational aspects. The findings of this study also indicate that senior business managers favoured a more vertical and bureaucratic organisational structure compared to the senior IT managers by placing less emphasis on operational staff for decision making for cyber crisis. However, seeking advice from IT employees for fast decision-making during cyber crisis was suggested by past studies, as noted in the literature review. The findings of this study reinforce the inclusion of both ecological and engineering resilience approaches in management decision making. This research appears to be one of the first to investigate the resilience approach in organisational cyber resilience.

Rather than focusing only on the senior IT manager role, this research investigated the role of business managers in strengthening organisational cyber resilience, as both managerial levels make decisions during cyber crisis. This research is among the first to consider the perspective

of business managers on cyber resilience development. The findings of this study demonstrated that the two senior management groups in the case studies do not share a common view on organisational cyber resilience. Business managers placed more emphasis on non-technical aspect of cyber resilience, while senior IT managers focused more on technical aspects. As a shared understanding of cyber resilience will benefit better strategic decision-making, the results of this research may assist managers and policymakers to be better informed about their key roles in developing a cyber-resilient organisation. As explained, greater communication between the two managerial levels may bring the business management perspective closer to the technical view (Rainer Jr et al., 2007). Increasing joint decision-making meetings between these two managerial levels, and providing practical examples of how cyber security tools and cyber resilience improvement can prevent adversaries from compromising organisational systems, may contribute to enhanced organisational cyber resilience. These actions may assist both business and IT managers to understand the role of each in building cyber resilience, resulting in benefit for organisations through protecting reputations and achieving strategic objectives.

This study points to a range of practical implications of the findings, in addition to extending the organisational and behavioural factors of the Matrix that influence cyber resilience. These implications include increasing organisational awareness of the criticality of involving both senior IT and business managers in all phases of the cyber resilience process. Such awareness will increasingly facilitate communication between, and training of, both groups to learn from past adverse events through joint review, and adaption to future events. This process may occur through the implementation of a restricted number of organisational policies that apply to the absorption, recovery and adaptation stages after a cyber incident, and not only in the planning stage.

As the case studies were restricted to two Australian universities, caution is needed before generalising the findings to other universities, large organisations or nations. This research offers a number of opportunities for further research, including comparative studies of senior IT and business manager perspectives of organisational cyber resilience in other nations and organisations including small and large, private and public and regional and metropolitan universities. This research identified that senior IT managers and business managers have different views on ecological and engineering resilience approaches. Another suggestion for future research is to investigate whether these diverse perspectives assist organisations to be more adaptive during an attack. A further avenue for research is to investigate the association between the type of resilience thinking that dominates an organisation, and whether the approach enables greater resilience.

References

ABC News. (2020). Scott Morrison's 'urgent' hacking warning shot shows Australia won't shy away from China's cyber attacks. Retrieved from https://www.abc.net.au/news/2020-06-20/why-australia-acted-on-china-hacking-cyber-attack-scott-morrison/12376700

Ahmad, A., Johnson, C., & Storer, T. (2015). An Investigation on Organisation Cyber Resilience *International Journal of Computer, Electrical, Automation, Control and Information Engineering, 9*, 1661-1666. Retrieved from http://www.waset.org/publications/10002012

Al-Surmi, A., Cao, G., & Duan, Y. (2020). The impact of aligning business, IT, and marketing strategies on firm performance. *Industrial Marketing Management, 84*, 39-49.

Alberts, D. S., Garstka, J. J., & Stein, F. P. (2000). *Network Centric Warfare: Developing and Leveraging Information Superiority*. Assistant Secretary of Defense (C3I/Command Control Research Program) Washington DC.

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. *Computers & Industrial Engineering, 149*, 106829.

Antikainen, J. (2014). *Model for national cybersecurity resilience and situation awareness improvement: An information quality–centric approach leveraging fusion of established practitioner and academic disciplines.* (Master Degree). Jamk University of Applied Science, Retrieved from https://www.theseus.fi/bitstream/handle/10024/86179/opinnaytetyo_%20Jani%20Antikainen.pdf?sequence=3

Appiah, G., Amankwah-Amoah, J., & Liu, Y.-L. (2020). Organizational Architecture, Resilience, and Cyberattacks. *IEEE Transactions on Engineering Management*.

Armstrong, C. P., & Sambamurthy, V. (1999). Information technology assimilation in firms: The influence of senior leadership and IT infrastructures. *Information Systems Research, 10*(4), 304-327.

Austin, G. (2018). *How Australian universities can get better at cyber security*. Retrieved from https://theconversation.com/how-australian-universities-can-get-better-at-cyber-security-99587#republish

Bagheri, S. (2020), Investigating Organisational Aspects of Cyber Resilience in Large Organisations, PhD thesis, University of Tasmania, Tasmania, Australia.

Bagheri, S., & Ridley, G. (2017). *Organisational cyber resilience: research opportunities.* Paper presented at the Proceedings of the 28th Australasian Conference on Information Systems (ACIS2017), Hobart, Australia.

Bei, H. (2019). *Problems of cybersecurity in the context of becoming and development of the new economy*. Collection of scientific works of the International Scientific Conference "Competitiveness and Innovation in the Knowledge Economy", XXI Edition, September 27-28, 2019, Chisinau, Moldova, e-ISBN 978-9975-75-968-7.

Bellini, E., & Marrone, S. (2020). *Towards a novel conceptualization of Cyber Resilience.* Paper presented at the 2020 IEEE World Congress on Services (SERVICES).

Béné, C., Newsham, A., Davies, M., Ulrichs, M., & Godfrey-Wood, R. (2014). Resilience, poverty and development. *Journal of International Development, 26*(5), 598-623.

Berg, B. L. (2004). *Qualitative Research Methods for the Social Sciences* (Vol. 5): Pearson Boston, MA.

Bergeron, F., Raymond, L., & Rivard, S. (2004). Ideal patterns of strategic alignment and business performance. *Information & Management, 41*(8), 1003-1020.

Berkes, F., Colding, J., & Folke, C. (2008). *Navigating social-ecological systems: building resilience for complexity and change*: Cambridge University Press.

Bernabe, J. B., & Skarmeta, A. (2019). Introducing the Challenges in Cybersecurity and Privacy-The European Research Landscape. *Challenges in Cybersecurity and Privacy-the European Research Landscape,* River Publishers Series in Security and Digital Forensics, 1-21.

Bernard, R. (2007). Information Lifecycle Security Risk Assessment: A tool for closing security gaps. *Computers & Security, 26*(1), 26-30.

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience–Fundamentals for a Definition. In *New Contributions in Information Systems and Technologies* (pp. 311-316): Springer.

Borys, S. (2019). The ANU hack came down to a single email—here's what we know. Retrieved from https://www.abc.net.au/news/2019-10-02/the-sophisticated-anu-hack-that-compromised-private-details/11566540

Buchmann, R. A., Polini, A., Johansson, B., & Karagiannis, D. (2020). *Perspectives in Business Informatics Research: 19th International Conference on Business Informatics Research, BIR 2020, Vienna, Austria, September 21–23, 2020, Proceedings* (Vol. 398): Springer Nature.

Burgemeestre, B., Hulstijn, J., & Tan, Y.-H. (2009). *Rule-based versus Principle-based Regulatory Compliance.* Paper presented at the JURIX.

Carias, J. F., Labaka, L., Sarriegi, J. M., & Hernantes, J. (2018). *An Approach to the Modeling of Cyber Resilience Management.* Paper presented at the 2018 Global Internet of Things Summit (GIoTS).

Cavelty, M. (2007). *Critical information infrastructure: vulnerabilities, threats and responses.* Paper presented at the Disarmament Forum (Vol. 3, pp. 15-22). UNIDIR.

Chapman, J., Chinnaswamy, A., & Garcia-Perez, A. (2018). *The severity of cyber attacks on education and research institutions: A function of their security posture.* Paper presented at the Proceedings of the13th International Conference on Cyber Warfare and Security (ICCWS 2018), Washington DC. USA.

Cobo, A., Vanti, A. A., & Rocha, R. (2014). A fuzzy multicriteria approach for it governance evaluation. *JISTEM-Journal of Information Systems and Technology Management, 11*, 257-276.

Colombo, R. (2020). *On the escalation from Cyber Incidents to Cyber Crises.* Master's thesis, University of Twente.

Conklin, W. A., & Kohnke, A. (2018). *Cyber Resilience: An Essential new Paradigm for Ensuring National Survival.* Paper presented at the Proceedings of the 13th International Conference on Cyber Warfare and Security (ICCWS 2018), Washington DC. USA.

Conklin, W. A., & Shoemaker, D. (2017). Cyber-Resilience: Seven Steps for Institutional Survival. *EDPACS, 55*(2), 14-22. Retrieved from http://www.tandfonline.com/doi/abs/10.1080/07366981.2017.1289026

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 4 (10): 13–21. In (Vol. 4, pp. 13–21).

Davis, J. I., Libicki, M. C., Johnson, S. E., Kumar, J., Watson, M., & Karode, A. (2016). *A Framework for Programming and Budgeting for Cybersecurity*. Retrieved from RAND Corporation, Santa Monica, CA, US.

Dewar, R. S. (2017). *Active Cyber Defense*. Retrieved from Center for Security Studies (CSS), ETH Zurich: https://doi.org/10.3929/ethz-b-000169631

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. J*ournal of Cybersecurity (Oxford)*, *5* (1), 1-17.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67-87. Retrieved from http://journals.sagepub.com/doi/pdf/10.2307/41166154

Feist, G. J. (2006). The development of scientific talent in Westinghouse finalists and members of the National Academy of Sciences. *Journal of Adult Development, 13*(1), 23-35.

Ferdinand, J. (2015). Building organisational cyber resilience: A strategic knowledge-based view of cyber security management. *Journal of Business Continuity & Emergency Planning, 9*(2), 185-195.

Fitzgerald, T. (2007). Clarifying the roles of information security: 13 questions the CEO, CIO, and CISO must ask each other. *Information Systems Security, 16*(5), 257-263.

Fox-Lent, C., Bates, M., & Linkov, I. (2015). A matrix approach to community resilience assessment: An illustrative case at Rockaway Peninsula. *Environment Systems and Decisions*, *35*(2), 209-218.

Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J., & Linkov, I. (2016). Resilience of Cyber Systems with Over-and Underregulation. *Risk Analysis, 37*(9), 1644–1651.

Goodman, PS., & Haisley, E. (2007). Social comparison processes in an organisational context: New directions. *Organisational Behavior and Human Decision Processes, 102(*1*),* 109-125.

Hambleton, R. K., Brennan, R. L., Brown, W., Dodd, B., Forsyth, R. A., Mehrens, W. A., . . . Linden, W. J. (2000). A response to "setting reasonable and useful performance standards" in the national academy of science'grading the nations report card. *Educational Measurement: Issues and Practice, 19*(2), 5-14.

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 100204.

Holling, C. (1996). Engineering resilience versus ecological resilience. *Engineering within Ecological Constraints, 31*(1996), 32.

Hult, F., & Sivanesan, G. (2014). What good cyber resilience looks like. *Journal of Business Continuity & Emergency Planning, 7*(2), 112-125.

Johnson, A. M. (2009). Business and security executives views of information security investment drivers: Results from a delphi study. *Journal of Information Privacy and Security, 5*(1), 3-27.

Kott, A., & Linkov, I. (2021). To improve cyber resilience, measure it. *arXiv preprint arXiv:2102.09455*.

Le, N. T., & Hoang, D. B. (2017). Capability Maturity Model and Metrics Framework for Cyber Cloud Security. *Scalable Computing: Practice and Experience, 18*(4), 277-290. doi:10.12694/scpe.v18i4.1329

Ligo, A., Kott, A. & Linkov, I. (2021). How to Measure Cyber Resilience of an Autonomour Agent: Approaches and Challenges, *IEEE Engineering Management Review*, 1-12.

Linkov, I., Eisenberg, D., Plourde, K., Seager, T., Allen, J., & Kott, A. (2013b). Resilience metrics for cyber systems. *Environment Systems & Decisions, 33*(4), 471-476. doi:http://dx.doi.org/10.1007/s10669-013-9485-y

Linkov, I., Senberg, D., Bates, M., Chang, D., Convertino, M., Allen, JH., Flynn, SE., & Seager, T. (2013a). Measurable Resilience for Actionable Policy. *Environmental Science & Technology, 47*(18), 10108-10110. doi:10.1021/es403443n

Linkov, I., & Trump, B. (2019). The Science and Practice of Resilience, *Cham: Springer International Publishing.*

Loonam, J., Zwiegelaar, J., Kumar, V., & Booth, C. (2020). Cyber-Resiliency for Digital Enterprises: A Strategic Leadership Perspective. *IEEE Transactions on Engineering Management*.

Luftman, J., Papp, R., & Brier, T. (1999). Enablers and inhibitors of business-IT alignment. *Communications of the Association for Information Systems, 1*(1), 11.

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018). *Implementing cyber-security measures in airports to improve cyber-resilience.* Paper presented at the Proceedings of the 2018 Global Internet of Things Summit (GIoTS), Bilbao, Spain.

Marchese, D., Jin, A., Fox-Lent, C. & Linkov, I. (2019). Resilience for Smart Water Systems, *Journal of Water Resources Planning and Management, 146*(1), 02519002.

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review, 31*(5), 622-660. doi:10.1108/14684520710832333

Merriam, S. B. (2009). Qualitative research: A guide to design and implementation: Revised and expanded from qualitative research and case study applications in education. San Franscisco: Jossey-Bass.

Moallem, A. (2020). *HCI for Cybersecurity, Privacy and Trust.* Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19-24, 2020, Proceedings (Vol. 12210): Springer Nature.

National Academy of Sciences. (2012). Disaster Resilience: A National Imperative Retrieved from https://www.nap.edu/read/13457/chapter/3

Noureddine, M. (2020). *Achieving network resiliency using sound theoretical and practical methods.* University of Illinois at Urbana-Champaign,

Orozco, J., Tarhini, A., & Tarhini, T. (2015). A framework of IS/business alignment management practices to improve the design of IT Governance architectures. *International Journal of Business and Management, 10*(4), 1.

Quacquarelli Symonds. (2018, 26 July 2018). Qs University Rankings. Retrieved from https://www.topuniversities.com/

Rainer Jr, R. K., Marshall, T. E., Knapp, K. J., & Montgomery, G. H. (2007). Do information security professionals and business managers view information security issues differently? *Information Systems Security, 16*(2), 100-108.

Rand, K, Kurth, M., Fleming, C., & Linkov, I. (2019). A resilience matrix approach for measuring and mitigating disaster-induced population displacement, *International Journal of Disaster Risk Reduction*, *42*(18), 101310.

Roege, P. E., Collier, Z. A., Chevardin, V., Chouinard, P., Florin, M.-V., Lambert, J. H., Nielsen, K., Nogal, M. and Todorovic, B. (2017). Bridging the Gap from Cyber Security to Resilience. In *Resilience and Risk* (pp. 383-414). NATO Science for Peace and Security Series C: Environmental Security: Springer.

Sabev, S. I. (2020). Integrated Approach to Cyber Defence: Human in the Loop. Technical Evaluation Report. *Information & Security: An International Journal*, *44*, 76-92.

Shapiro, S., Keys, B., Chhajer, A., Liu, Z., & Horner, D. (2016). *A Framework for Assessing Cyber Resilience*. A Report for the World Economic Forum.

Sarkar, A., Wingreen, S., & Cragg, P. (2013). *Organisational IS Resilience: a pilot study using Q-methodology.* Paper presented at the 24th Australasian Conference on Information Systems (ACIS2013).

Segovia, M., Rubio-Hernan, J., Cavalli, A. R., & Garcia-Alfaro, J. (2020). *Cyber-Resilience Evaluation of Cyber-Physical Systems.* Paper presented at the 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA).

Selby, J. (2017). How Can Company Boards Build Trust When Faced By Cybersecurity Risks? *Optus Macquarie University Cyber Security Hub*, 3. Retrieved from https://www.mq.edu.au/about/about-the-university/offices-and-units/optus-macquarie-university-cyber-security-hub/news2/files/Boards-Building-Trust-Cyber-Security-Hub-John-Selby.pdf

Sepúlveda-Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers & Security*, 101996.

Sharma, R. (2015). Five ways board members can improve cybersecurity. *Journal of Internet Law, 19*(4), 11-12.

Sikula, N., Mancillas, J., Linkov, I., & McDonagh, J. (2015). Risk management is not enough: a conceptual model for resilience and adaptation-based vulnerability assessments. *Environment Systems & Decisions, 35*(2), 219-228. doi:http://dx.doi.org/10.1007/s10669-015-9552-7

Smith, A. E., & Humphreys, M. S. (2006). Evaluation of unsupervised semantic mapping of natural language with Leximancer concept mapping. *Behavior Research Methods, 38*(2), 262-279.

Soomro, Z. A., Mahmood, H. S., & Javed, A. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215-225.

Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST Special Publication, 800*(82), 16-16.

Tallon, P. P. (2014). Do you see what I see? The search for consensus among executives' perceptions of IT business value. *European Journal of Information Systems, 23*(3), 306-325.

Teo, T. S., & King, W. R. (1997). An assessment of perceptual differences between informants in information systems research. *Omega, 25*(5), 557-566.

Tisdale, S. M. (2016). Architecting a cybersecurity management framework. *Issues in Information Systems, 17*(4), 227-236. Retrieved from http://www.iacis.org/iis/2016/4_iis_2016_227-236.pdf

Trim, P., Jones, N., & Brear, K. (2009). Building organisational resilience through a designed-in security management approach. *Journal of Business Continuity & Emergency Planning, 3*(4), 345-355.

van der Kleij, R., & Leukfeldt, R. (2019). *Cyber resilient behavior: Integrating human behavioral models and resilience engineering capabilities into cyber security.* Paper presented at the Proceedings of the International Conference on Applied Human Factors and Ergonomics, Advances in Human Factors in Cybersecurity (AHFE), Washington DC. USA.

Vugrin, E., & Turgeon, J. (2013). Advancing Cyber Resilience Analysis with Performance-Based Metrics from Infrastructure Assessments. *International Journal of Secure Software Engineering (IJSSE), 4*(1), 75-96.

Wagstaff, K., & Sottile, C. (2015). *Cyberattack 101: Why Hackers Are Going After Universities*. Retrieved from http://www.nbcnews.com/tech/security/universities-become-targets-hackers-n429821

Wang, N., Liang, H., Zhong, W., Xue, Y., & Xiao, J. (2012). Resource structuring or capability building? An empirical study of the business value of information technology. *Journal of Management Information Systems, 29*(2), 325-367.

Wells, E., Boden, M., Tseytlin, I & Linkov, I. (2022). Modeling Critical Infrastructure Resilience under Compounding Threats: A systematic literature review. *Progress in Disaster Science*, *15*, 1-15.

White, G. (2009). Strategic, tactical, & operational management security model. *Journal of Computer Information Systems, 49*(3), 71-75.

Yano, E., de Abreu, W., Gustavsson, P., & Åhlfeldt, R. (2015). *A framework to support the development of Cyber Resiliency with Situational Awareness Capability.* Paper presented at the Proceedings of the 20th International Command and Control Research and Technology Symposium, Annapolis, MD, USA.

Appendix A: Interviews cited

To respect participant confidentiality, the authors did not disclose interviewee job titles. Only broad areas of responsibility have been provided in the following:

Interviewee 1: Business manager, Human Resources, 20 years of experience, C1U, [interview date: 20 June 2018].

Interviewee 2: Business manager, Finance Operations, 22 years of experience, C1U, [interview date: 15 June 2018].

Interviewee 3: Business manager, Risk Area, 11 years of experience, C1U, [interview date: 14 June 2018].

Interviewee 4: Business manager, Business Operations, 28 years of experience, C1U, [interview date: 20 August 2018].

Interviewee 5: Business manager, Budget Allocation, 21 years of experience, C1U, [interview date: 11 December 2017].

Interviewee 6: IT senior manager, Strategy Design, 20 years of experience, C1U, [interview date: 9 January 2018].

Interviewee 7: IT senior manager, Enterprise Architecture, 23 years of experience, C1U, [interview date: 1 June 2018].

Interviewee 8: IT senior manager, IT Improvement, 26 years of experience, C1U, [interview date: 27 September 2017].

Interviewee 9: IT senior manager, Security Management, 21 years of experience, C1U, [interview date: 17 January 2018].

Interviewee 10: Business manager, Human Resources, 18 years of experience, C2U, [interview date: 18 June 2018].

Interviewee 11: Business manager, Finance Operations, 11 years of experience, C2U, [interview date: 26 June 2018].

Interviewee 12: Business manager, Business Operations, 22 years of experience, C2U, [interview date: 14 June 2018].

Interviewee 13: IT senior manager, Strategy Design, 22 years of experience, C2U, [interview date: 5 October 2017].

Interviewee 14: IT senior manager, Infrastructure Services, 26 years of experience, C2U, [interview date: 12 June 2018].

Interviewee 15: IT senior manager, IT Improvement, 26 years of experience, C2U, [interview date: 13 June 2018].

Interviewee 16: IT senior manager, Security Management, 22 years of experience, C2U, [interview date: 13 June 2018].

Interviewee 17: IT senior manager, Technology Application, 17 years of experience, C2U, [interview date: 14 June 2018].

doi: https://doi.org/10.3127/ajis.v27i0.4183