2017

Organisational Cyber Resilience: research opportunities

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

Gail Ridley
University of Tasmania, Gail.Ridley@utas.edu.au

Organisational Cyber Resilience: Research opportunities

Seyedehsaba Bagheri
Tasmanian School of Business & Economics
University of Tasmania
Hobart, Tasmania
Email: seyedehsaba.bagheri@utas.edu.au

Gail Ridley
Tasmanian School of Business & Economics
University of Tasmania
Hobart, Tasmania
Email: gail.ridley@utas.edu.au

Abstract

Cyber resilience has emerged as a new discipline to help organisations deal with cyber problems that cannot be addressed by traditional cyber security solutions. This study analysed the scattered literature on organisational aspects of cyber resilience using Linkov et al.'s (2013a) framework for cyber resilience. Three approaches were identified among the studies. This research found that limited investigation into organisational cyber resilience has been undertaken, while organisational aspects of cyber resilience have received less attention when compared to technical topics. The findings challenge the passive assumption of cyber resilience that appears to underlie many of the publications, which followed a cyber security approach. The limited work found, gaps in research subtopics and the underlying assumptions of organisational cyber-resilience, all point to research opportunities for researchers.

Keywords (Organisational cyber resilience, research opportunities, cyber resilience publications, past trends)

1 Introduction

The business activities of organisations largely rely on cyber activity, arising from advancements in information technology and telecommunication networks. Organisations' needs for cyber infrastructure to meet information and commercial objectives have expanded dramatically over past decades (Tran et al. 2016). Cyber related issues create problems for organisations around the world for international trade, service efficiency and the marketing of commodities. The high cost of cyber-attacks creates problems for organisations and their clients. As new forms of cyber-attacks evolve, both public and private organisations are targeted. A common purpose of cyber-attacks is to gain access to confidential information, because information is an important organisational asset that may endanger the organisation if disclosed (Tran et al. 2016).

The scope of the present study is limited to cyber resilience instead of cyber security. While cyber security experts attempt to establish best practice standards and principles to improve cyber security, such guidelines are inadequate to address information security problems (Hult and Sivanesan 2014). Organisations need to adopt a resilience approach to cyber security, rather than merely implement cyber security controls (Christou 2016). The term resilience refers to the capacity of systems to cope with, adapt to, and recover from, disturbance (Lei et al. 2014). The concepts of cyber security and resilience differ. As cyber security consists of the procedures and measures taken to keep information, and computer systems, safe, it focuses on restricting data access to minimise information risk (Antikainen 2014). In contrast, cyber resilience is the capacity of a cyber-system to perform effectively regardless of hazards in the business environment. Many organisations realize that cyber security programs without cyber resilience cannot minimise their cyber dangers (Bindiya 2016; Bodeau and Graubart 2011). Cyber security seeks stability and to reduce disturbance, but in today's complex environment there is no guarantee of organisational stability. Cyber resilience researchers argue instead that instability is a characteristic of cyber space (Chandler 2014; Kaufmann 2015).

The majority of the studies undertaken in the cyber resilience area consider technical aspects, while few studies investigate organisational aspects of cyber resilience. However, cyber resilience includes both technical and organisational elements (Nicholas 2016). Ten years of research demonstrate that major cyber incidents arise from human errors, rather than from technical problems (Stolfo et al. 2008). Moreover, Arce (2003) reported the greatest risks to information systems stem from human beings, and not from technical problems. A lack of academic research that investigates organisational aspects of cyber resilience may lead to problems for the business environment, if companies are not aware of how organisational factors may influence their cyber resiliency.

This paper conducts a comprehensive review of the extant literature on organisational aspects of cyber resilience. It will integrate the information presented in the fragmented resources available, using a cyber resilience framework (Linkov et al. 2013a) to analyse the nature of publications in the area. Just 36 papers were found that specifically referred to organisational aspects of cyber resilience. The results of this investigation provide direction to future researchers on the current body of knowledge for organisational cyber resilience, its limitations, and opportunities for future research.

Section 2 explains the cyber resilience concept further, and the importance of organisational aspects of cyber resilience. Section 3 reviews previous studies on organisational aspects of cyber resilience. Section 4 discusses the Linkov et al. (2013a) framework, while Section 5 presents the methodology used to identify and analyse the literature for this study. Then Section 6 analyses the nature of past studies, using the Linkov et al. (2013a) framework, before presenting the results and discussion. Section 7 contains the study's conclusions, limitations and contributions to research and practice, with suggestions for future research into organisational aspects of cyber resilience.

2 Cyber Resilience in an Organisational Context

Cyber resilience has been regarded as one of the most important business objectives (Geers 2009). It contributes to improving the functionality of companies and societies worldwide (Ferdinand 2015).

All organisational operations and information structures that rely on digital communication systems require the capability to withstand cyber crises (Bodeau and Graubart 2011). To protect the privacy of organisations' information, cyber security experts impose policies and procedures to restrict data access and minimise risk, often following guidelines from external experts. However, cyber security relies on a passive system defence in comparison to cyber resilience (Chandler 2014; Kaufmann 2015). As cyber resilience focuses on the capacity of organisations to perform effectively regardless of business environment hazards, continuous communication between a disturbance and the reaction is

required (Chandler 2014). Therefore cyber resilience depends on an active response (Chandler 2014; Kaufmann 2015), and is different to cyber security.

Cyber resilience is seen as a system's capability to "anticipate, withstand, recover from, and adapt" to changing environments and vulnerable situations (Bodeau and Graubart 2011). In a second related view, some researchers see the purpose of cyber resilience is to assist organisations to operate in different conditions (Geers 2009). From this latter perspective, cyber resilience helps organisations to learn from adverse circumstances (Hult and Sivanesan 2014). However, a third view of cyber resilience argues that it is about returning to the original situation after disturbance (Williams and Manheke 2010). The current study adopts the first and second views of cyber resilience as outlined above.

Increased attention has been paid to cyber resilience recently (Ferdinand 2015). While establishing cyber resilience procedures in an organisation is an essential aim of business communities, it is hard to accomplish (Ferdinand 2015). Cyber resilience needs to concentrate on organisational and cultural issues as much as technical issues (Nicholas 2016). However, the scholarly literature on organisational aspects of cyber resilience is both limited and not well organised (Ferdinand 2015). There is no generally accepted and practical method for cyber resilience assessment in organisations. The limited literature and its lack of integration decreases opportunities for organisations to develop and implement cyber resilience (Ferdinand 2015), and for researchers to extend knowledge in the area.

Although there is no doubt that organisations need to acquire further knowledge in the technical aspects of cyber resilience, developing understanding of the organisational aspects is required. The organisational aspects of cyber resilience that are relevant to business operations are expected to cover a broader area than the technical aspects. Moreover, technical knowledge may be limited to specific aspects of a system, and not consider other important system layers, including the social, information and cognitive layers (Linkov et al. 2013b). The next section will review the existing literature on cyber resilience from an organisational context.

3 Previous Studies on Organisational Cyber Resilience

This paper aims to identify the nature of past studies on organisational aspects of cyber resilience. As stated, many papers published in this new area considered only its technical aspects. As examples, both the Cyber Resilience Recovery Model (Tran et al. 2016) and the elements of cyber resilience identified by Thebeau II et al. (2014), proposed solutions to improve the technical aspects of cyber resilience. As the scope of this study is limited to organisational aspects of cyber resilience, this paper does not examine technical cyber resilience publications. A limited number of academic publications was noted, primarily derived from beginning research into organisational aspects of cyber resilience (Björck et al. 2015). Consequently, both academic and practitioner resources were investigated.

There is an extensive literature on resilience, while the term has been used since the 1950s in the same way as in this study. As the term resilience has high recognition by researchers, and is used in a specific way in this investigation, the decision was made not to include the broader Information Systems or information security literature unless the search terms identified relevant studies. The following review discusses the current literature in the area.

Interest in examining organisational aspects of cyber resilience began only recently. One of the first studies in the area was carried out by the World Economic Forum in 2012, which collated knowledge on cyber resilience. The World Economic Forum report (2012) contained recommendations for improving cyber resilience, including the need to consider stakeholders and the importance of management and leadership positions. Since 2012, additional recommendations for cyber resilience have emphasised the role of staff members (ANAO 2016), including through enhanced information sharing and the creation of learning environments (ASIC 2016; Bindiya 2016; Dalton et al. 2017; Davis 2015; Davis et al. 2016; Ferdinand 2015; Hult and Sivanesan 2014; Putranti 2015), collaboration among staff members (ANAO 2016; ASIC 2016; Hult and Sivanesan 2014; Shapiro et al. 2016) and the significance of training programs (ANAO 2016; ASIC 2016; Dalton et al. 2017; Ferdinand 2015; Hult and Sivanesan 2014; Shapiro et al. 2016).

Other authors also studied the role of managers and leaders in promoting cyber resilience (ANAO 2016; Dalton et al. 2017; Hult and Sivanesan 2014; Ingram and Martin 2017; Sarkar et al. 2013; Shapiro et al. 2016). All these authors suggested that where a senior manager or leader undervalued cyber resilience, other staff may take this viewpoint in the long-term. The thrust of many of these publications was that it is not appropriate to expect IT technical people to accept responsibility for cyber incidents. Leaders and managers must accept responsibility as well.

Other management influences on cyber resilience identified in the literature included developing a security culture (CPMI 2014; North and Pascoe 2016), the need for recovery and response planning (ASIC 2015; ASIC 2016; Bindiya 2016; Bodeau and Graubart 2016a; Bodeau and Graubart 2016b; Dalton et al. 2017; Shapiro et al. 2016), and the contribution of cyber governance and monitoring programs (ASIC 2015; ASIC 2016; Davis 2015; Ferdinand 2015; North and Pascoe 2016). Another management role proposed to strengthen cyber resilience was the selection and application of appropriate rules in organisations to decrease cyber risks and increase cyber resilience (Putranti 2015).

Some studies emphasised cyber resilience operational issues in organisations, including defining asset management processes to access computer system records, networks, data and other information resources from inside or outside (ASIC 2015; ASIC 2016; Bodeau and Graubart 2016b; Dalton et al. 2017; Davis et al. 2016; Ingram and Martin 2017). Other authors focused on risk assessment programs, as did the World Economic Forum (2012) and the CPMI (2014). Other research considered assurance procedures, including testing programs (Joiner 2017) and use of the cyber exercise method (Hult and Sivanesan 2014; Shapiro et al. 2016). Publications also highlighted the importance of documenting all cyber resilience procedures and related issues (Ingram and Martin 2017; Shapiro et al. 2016). A further consideration proposed that may influence cyber resilience programs was to examine organisational communications with third parties (Putranti 2015; Shapiro et al. 2016).

From an examination of the literature, it appears that the studies followed three main approaches to consider cyber resilience in an organisational context:

Approach 1: Studies that attempted to provide an evaluation tool to identify a level of cyber resilience in organisations. The World Economic Forum (2012) first proposed identifying the cyber resilience maturity level of organisations, an approach that was then followed by Ferdinand (2015) and the ANAO (2016).

Approach 2: Studies that proposed other recommendations to improve organisational cyber resilience programs. They varied from suggesting good practices and principles ASIC 2016), to designing checklist programs. The World Economic Forum (2012), developed a c-suite checklist for organisational cyber resilience, an approach continued by Hult and Sivanesan (2014) and ASIC (2015).

Approach 3: Studies that proposed organisational factors to contribute to cyber resilience, either structured into a matrix or not. Some used a matrix to suggest cyber resilience metrics. One study proposed cyber resilience metrics based on different system layers (Linkov et al. 2013a) to develop an organisational cyber resilience matrix. While earlier authors had collated metrics for cyber resilience, they considered only the technical aspects (see Bodeau et al. 2012). Shapiro et al. (2016) refined the Linkov et al. (2013a) cyber resilience matrix for organisations, using system layers. Additional studies identified organisational factors that contribute to cyber resilience, but without using a structured matrix approach (Bindiya 2016; Christou 2016; CPMI-IOSCO 2015; Dalton et al. 2017; Davis et al. 2016; Hiller and Russell 2015; Joiner 2017; Kaufmann 2015; North and Pascoe 2016).

The cyber resilience matrix to examine organisational cyber resilience, as introduced in Approach 3 above (Linkov et al. 2013a), will be discussed next.

4 Linkov et al.'s (2013) Framework

This section introduces Linkov et al.'s (2013a) cyber resilience matrix, a "4 X 4" framework that will be used later to analyse the organisational cyber resilience literature. Linkov et al. (2013a) used the operational domains defined by the Doctrine of Network Centric Warfare (NCW) for the vertical axis, claiming that cyber resilience functionality depends on system performance throughout all operational domains. The four domains of Linkov et al. (2013a)'s framework are:

- Physical: Different physical assets of the organisation;
- Information: Accurate information about the physical assets;
- Cognitive: The decision-making process based on the physical and information layers, and
- Social: Having communications for taking decisions (Linkov et al. 2013a).

Linkov et al. (2013b) also integrated the four stages of event management described by the National Academy of Sciences (NAS) into the horizontal axis of their framework: plan/prepare, absorb, recover and adapt. Each cell of the resilience matrix identifies the capacity of a system for cyber resilience at each NCW domain, and applies it to the decision-making processes listed by NAS.

The cyber resilience matrix of Linkov et al. (2013a) was selected to analyse the nature of organisational cyber resilience publications for several reasons: 1) It integrates four domains of resilience with four stages of decision making. The design of the matrix reflects a definition of cyber resilience that incorporates the need to plan, absorb, recover, and adapt (Bodeau and Graubart 2011; Williams and Manheke 2010; World Economic Forum 2012). Choosing a framework that incorporates multiple organisational domains will enable a more detailed analysis of the studies, by attempting to identify their focus and processes. 2) Based on a definition of resilience that considers a system's capacity to withstand disruption (Lei et al. 2014), it is relevant to evaluate whether past research considers actions to be performed after disruption, or only examines the avoidance and minimisation of disruptions. The cyber resilience matrix also considers system capability when disruptions happen in the Absorb/Recovery/Adapt phases. These features of the Linkov et al. (2013a) matrix provide this study an opportunity to assess which aspects of cyber resilience were considered in the previous studies. 3) Linkov et al. (2013a)'s cyber resilience matrix is the only academic cyber resilience framework identified to consider the information, cognitive and social domains of cyber resilience, rather than focusing only on the technical aspects. It is also the only cyber resilience matrix found that maps the domains to the NAS event management stages.

Neither of the two other academic frameworks published on organisational cyber resilience are suitable for this study. Ferdinand (2015) proposed different knowledge levels of cyber resilience in organisations. The Information Systems resilience conceptual model by Sarkar et al. (2013) concentrates on the external and internal elements that influence information system resilience in organisations. Neither framework appears to reflect the definition of resilience used in this current study regarding adapting to change. The following section discusses the methodology for this study.

5 Methodology

The aim of this study is to investigate the conceptual nature of published research on organisational aspects of cyber resilience, by conducting a comprehensive review of its literature. As explained, the cyber resilience matrix by Linkov et al. (2013) will be used for this task.

The methodology is illustrated in Figure 1. This study first identified both academic and practitioner publications on the topic, as academic papers appeared limited. Publications were identified and collated from sources that included journal databases, books, theses, organisational, governmental, industry and technical reports, and research and professional websites. All non-academic publications were considered as "practitioner". The search terms were "cyber resilience", "organisational cyber resilience", "organisational resilience", "cyber security resilience" and "cyber resilience in organisation", and variants. The search to August 2017 was not limited by time period. Technical publications were excluded where they did not also discuss any organisational aspects. A summary was prepared of any organisational cyber resilience components mentioned. Papers were excluded where organisational components were not found in the screening procedure.

The vertical domains of Linkov et al.'s (2013) cyber resilience matrix were used to categorise the identified publications into physical, information, cognitive and social domains (Table 6). Frequencies were recorded by domain for the publications, and whether academic or researcher-oriented.

The horizontal elements of the Linkov et al. (2013) matrix were used to categorise each identified publication into the plan/prepare, absorb, recover and adapt stages (Table 6). A record was made of publication frequencies in each category, and whether the papers were academic or researcher-oriented.

Two researchers coded the publications independently using the same framework. The inter-rater reliability was calculated using Krippendorff's Coefficient. The study's results, and discussion, are presented in the next section.

6 Results and Discussion

As can be seen in Table 1, 450 academic and practitioner publications were reviewed to identify those that considered organisational aspects of cyber resilience. Only 36 were found to be relevant. The remaining 414 publications focused on either technical aspects of cyber resilience, or organisational aspects of resilience, without considering the cyber domain. Many of the publications examined focused on cyber security issues, without discussion of the resilience aspects. Table 1 indicates that practitioners (55%) accounted for more of the publications on organisational cyber resilience than academics (44%). Rounding errors account for the discrepancy in the percentages.

Publications on organisational cyber resilience increased between 2012 and the end of July 2017 (see Table 2 and Table 3), after the first publication was noted in 2012. Percentages were used to enable easier comparison. Publications that were categorised into Linkov et al.'s (2013) physical, information, cognitive and social domains, and their plan/prepare, absorb, recovery and adapt stages, accounted for a small percentage of the 36 papers until 2014 (see Table 2 and 3). In 2015 the percentage of relevant publications started to increase, most noticeably in the cognitive and social domains, and for the plan/prepare phase. The increased proportion of publications continued in 2016. The limited publications identified, their recency and the pattern of increase indicates that interest in the organisational aspects of cyber resilience is new and growing.

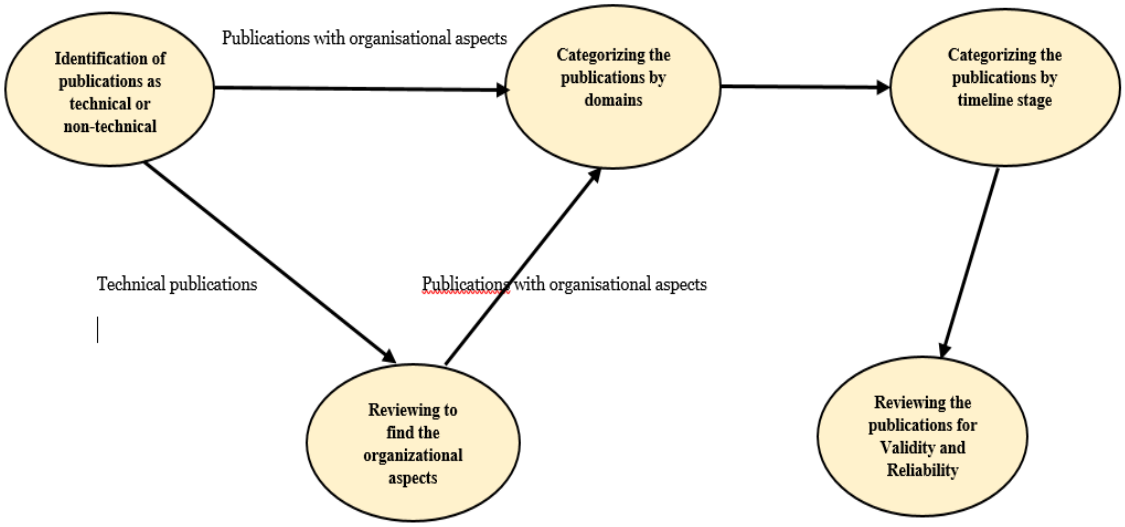

Figure 1: The process used for analysis of past studies

Total papers	*Relevant papers*	*(Academic papers)*	*(Practitioner papers)*
450	36	16 [44%]	20 [55%]

Table 1. Total reviewed papers, and relevant publications categorised as academic or practitioner

Domains	2012	2013	2014	2015	2016	2017 (To August)
Physical	0%	5%	8%	19%	25%	13%
Information	0%	0%	8%	22%	25%	5%
Cognitive	2%	5%	8%	25%	25%	11%
Social	2%	2%	8%	25%	30%	5%

Table 2. Percentage of total relevant papers for the domains by year

Stages	2012	2013	2014	2015	2016	2017 (To August)
Plan/ prepare	2%	5%	8%	25%	27%	16%
Absorb	2%	5%	8%	13%	30%	2%
Recovery	0%	2%	8%	16%	19%	8%
Adapt	0%	0%	5%	13%	16%	2%

Table 3. Percentage of total relevant papers for the stages by year

A breakdown of analysis of the relevant publications by domain (Table 4) and stage (Table 5) using Linkov et al.'s (2013a) cyber resilience framework appears below for author category. When categorising the publications into the physical, information, cognitive and social domains (Table 4), a greater percentage of both author groups focused on cognitive issues of cyber resilience. Less attention was paid to issues in the information domain of organisational cyber resilience in comparison to the other domains. Note that many publications were categorised into more than one domain, or stage.

Domains	Academic studies	Practitioner studies	Total studies
Physical	22%	44%	66%
Information	19%	41%	60%
Cognitive	33%	47%	80%
Social	27%	47%	74%

Table 4. Percentage of relevant academic and practitioner publications by framework domains

After categorising the relevant publications into the four event management stages from the framework (Table 5), the results show a higher percentage of the publications appeared in the plan/prepare stage (90%) when compared to the other three stages. Less attention was paid to the organisational capability to withstand after a disruption, that is, to each of the Absorb/Recovery/Adapt stages, for both academic and practitioner work. The adaptation stage received the least attention.

Stages	Total academic's studies	Total practitioner's studies	Total studies
Plan/ prepare	38%	52%	90%
Absorb	25%	38%	63%
Recovery	22%	33%	55%
Adapt	8%	30%	38%

Table 5. Percentage of relevant academic and practitioner publications by framework stages

	Plan/ prepare for	Absorb	Recover from	Adapt to
Physical	Practitioner:14 Academic:9 Total: 23 (64%)	Practitioner:9 Academic:1 Total: 10 (27%)	Practitioner:8 Academic:5 Total:13 (36%)	Practitioner:10 Academic:3 Total:13 (36%)
Information	Practitioner:14 Academic:6 Total: 20 (55%)	Practitioner:6 Academic:4 Total:10 (27%)	Practitioner:8 Academic:1 Total:9 (25%)	Practitioner:5 Academic:1 Total:6 (16%)
Cognitive	Practitioner:16 Academic:9 Total: 25 (69%)	Practitioner:11 Academic:5 Total: 16 (44%)	Practitioner:10 Academic:2 Total:12 (33%)	Practitioner:6 Academic:1 Total:7 (19%)
Social	Practitioner: 17 Academic:10 Total: 27 (75%)	Practitioner:9 Academic:3 Total: 12 (33%)	Practitioner:8 Academic:5 Total:13 (36%)	Practitioner:6 Academic:2 Total:8 (22%)

Table 6. Publication frequencies, categorised by cell, using Linkov et al.'s (2013a) cyber resilience matrix (note that the same publication may appear in more than one cell).

The frequency of the 36 publications with an organisational cyber resilience focus, categorised into one or more of the cells of the Linkov et al.'s (2013a) matrix, and for each author group, appear in

Table 6. It can be seen that the matrix cells appear at the intersection of the domains and event management stages. The percentages are of the 36 papers.

From the analysis in Table 6, the cell at the intersection of the plan/prepare stage of the event management and the social domain, contained the highest number of publications with 27 (75%) of the total. The next highest was for the cell that intersects the plan/prepare stage and the cognitive domain, with 25 papers, or 69% of the total. The cells that intersected the plan/prepare stage and the physical domain, and the plan/prepare stage and the information domain, had the next highest publications, with 23 (64%) and 20 (55%) of the total number publications, respectively. The lowest number of publications categorised using the matrix came from the adapt stage, with eight (22%) from the social, seven (19%) from the cognitive and six (16%) from the information domains.

As explained, the results of categorising relevant past publications reveal that the major focus of the papers published in the area of organisational cyber resilience is on planning and preparing for social-related activities. The findings reveal that the past publications focused least on the adaptation stage of cyber resilience, for the information domain.

These results suggest a range of implications for research into cyber resilience in organisations. First, while all 36 publications considered organisational cyber resilience, many appeared to incorporate a passive cyber security approach, rather than the active resilience approach. Cyber security scholars often focus on decreasing cyber threats, while cyber resilience necessitates a continuous communication between a disturbance and a reaction (Chandler 2014). The results of the analysis suggest that the identified publications placed most focus on the plan/prepare stage to minimise cyber risk, which is an approach suggestive of cyber security. This finding implies that many cyber resilience publications are underpinned by a passive interpretation of cyber resilience, instead of a more active meaning. Therefore, authors publishing in the area of cyber resilience are urged to reflect on, and clarify their understanding of cyber resilience, and differentiate between cyber security and cyber resilience. Research that adopts the active concept of cyber resilience, and investigates how organisations absorb, recover from, and in particular adapt to, cyber threat, will be best placed to contribute to the future body of knowledge in this area.

Overall interest in the organisational aspects of cyber resilience increased during the five years since 2012. However, while focus on the physical areas of organisational cyber resilience grew, attention to social and behavioural issues declined. This finding suggests that an increased proportion of those who became interested in organisational cyber resilience in very recent years preferred to seek solutions from the physical domain. Opportunities also exist for researchers to address cyber threat problems by positioning their work in the information, cognitive and social perspectives.

The final adaptation stage of the four event management stages of the framework had the smallest number of publications for all five years. Adaptation received the least attention among academics. Adaptation and adjustment to external threats are fundamental to resilience, and require a system to have the capacity to adjust to a new situation (Berkes et al. 2008). There is a perspective on resilience that seeks a system to return to its original state after a shock, without the need to adapt to a new position (Grimm and Wissel 1997; Holling 1996). However maintaining stability in cyber systems will not enable organisations to address new and changing cyber threats. Opportunities exist for academic researchers to investigate how organisations may adapt to become cyber resilient. It is possible that once organisations learn to adapt to a cyber threat, they will become better able to adapt to different cyber threats in the future. Research into ways for organisations to adapt to build cyber resilience will also contribute to practice by offering guidance arising from academic research. Specifically, researchers are encouraged to consider organisational adaption for cyber resilience in the information domain, a neglected area of study.

7 Conclusion

This paper analysed the nature of past publications on organisational cyber resilience. It presented a literature review of this new field, in an area that has caught the interest of media, governments and business in current times. This study integrated information presented in the fragmented resources available, and appears to be the first investigation to review the literature in the area. A framework by Linkov et al. (2013a) was used to analyse the nature of both academic and practitioner publications on organisational cyber resilience. The publications were analysed using the four framework domains, physical, information, cognitive and social, and the management stages of plan/prepare, absorb, recover from, and react to.

While the number of publications used was limited, the specificity of the terms used by researchers in this area enabled the search to be comprehensive, within the study's scope. The results of this study have implications for both academics and practitioners by pointing to opportunities and needs for organisational cyber resilience research, from the results of analysis. This study also comments on some recent attempts to investigate organisational cyber resilience, by pointing to inconsistencies in the underlying assumptions of some of that work.

8 References

ANAO. 2016. "Cyber Resilience across Entities", 37, Australian National Audit Office, Canberra ACT.

Arce, I. 2003. "The Weakest Link Revisited [Information Security]", IEEE Security & Privacy (99:2), pp 72-76.

ASIC. 2015. "Cyber Resilience: Health Check", 429, Australian Securities and Investments Commission (ASIC), p. 67.

ASIC. 2016. "Cyber Resilience Assessment Report: ASX Group and Chi-X Australia Pty Ltd", 468, (ASIC) Australian Securities and Investments Commission p. 25.

Berkes, F., Colding, J., and Folke, C. 2008. Navigating Social-Ecological Systems: Building Resilience for Complexity and Change. Cambridge University Press.

Bindiya, T. 2016. "Resilience -- the Solution to Cyber Terrorism?", Military Technology (40 7/8), p 2.

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

Bodeau, D., and Graubart, R. 2011. "Cyber Resiliency Engineering Framework", MTR110237, MITRE Corporation).

Bodeau, D., and Graubart, R. 2016a. "Cyber Resilience Metrics: Key Observations".

Bodeau, D., and Graubart, R. 2016b. "Structured Cyber Resiliency Analysis Methodology (Scram)".

Bodeau, D., Graubart, R., LaPadula, L., Kertzner, P., Rosenthal, A., and Brennan, J. 2012. "Cyber Resiliency Metrics, Version 1.0, Rev. 1," The MITRE Corp, Bedford, MA, MP120053, Rev, 1.).

Chandler, D. 2014. Resilience: The Governance of Complexity. Routledge.

Christou, G. 2016. Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy. Springer.

CPMI-IOSCO. 2015. "Guidance on Cyber Resilience for Financial Market Infrastructures", Bank for International Settlements and International Organisation of Securities Commissions p. 30.

CPMI. 2014. "Cyber Resilience in Financial Market Infrastructures", Bank for International Settlements, p. 19.

Dalton, W., Van Vuuren, J.J., and Westcott, J. 2017. "Building Cybersecurity Resilience in Africa," ICMLG2017 5th International Conference on Management Leadership and Governance: Academic Conferences and publishing limited, p. 112.

Davis, A. 2015. "Building Cyber-Resilience into Supply Chains," Technology Innovation Management Review (5:4), p 19.

Davis, J., Libicki, M.C., Johnson, S.E., Kumar, J., Watson, M., and Karode, A. 2016. "A Framework for Programming and Budgeting for Cybersecurity", Santa Monica, Calif.

Ferdinand, J. 2015. "Building Organisational Cyber Resilience: A Strategic Knowledge-Based View of Cyber Security Management," Journal of business continuity & emergency planning (9:2), pp 185-195.

Geers, K. 2009. "The Cyber Threat to National Critical Infrastructures: Beyond Theory", Information Security Journal: A Global Perspective (18:1), pp 1-7.

Grimm, V., and Wissel, C. 1997. "Babel, or the Ecological Stability Discussions: An Inventory and Analysis of Terminology and a Guide for Avoiding Confusion", Oecologia (109:3), pp 323-334.

Hiller, J., and Russell, R. 2015. "Modalities for Cyber Security and Privacy Resilience: The NIST Approach", Proceedings of the 12th International Conference on Information Systems for Crisis Response and Management, Kristiansand, Norway.

Holling, C. 1996. "Engineering Resilience Versus Ecological Resilience", Engineering within ecological constraints (31:1996), p 32.

Hult, F., and Sivanesan, G. 2014. "What Good Cyber Resilience Looks Like", Journal of business continuity & emergency planning (7:2), pp 112-125.

Ingram, M., and Martin, M. 2017. "Guide to Cybersecurity, Resilience, and Reliability for Small and under-Resourced Utilities", National Renewable Energy Lab. (NREL), Golden, CO (United States).

Joiner, K.F. 2017. "How Australia Can Catch up to U.S. Cyber Resilience by Understanding That Cyber Survivability Test and Evaluation Drives Defense Investment", Information Security Journal: A Global Perspective), pp 1-11.

Kaufmann, M. 2015. "Resilience Governance and Ecosystemic Space: A Critical Perspective on the EU Approach to Internet Security", Environment and Planning D: Society and Space (33:3), pp 512-527.

Lei, Y., Yue, Y., Zhou, H., and Yin, W. 2014. "Rethinking the Relationships of Vulnerability, Resilience, and Adaptation from a Disaster Risk Perspective", Natural hazards (70:1), pp 609-627.

Linkov, I., Eisenberg, D., Plourde, K., Seager, T., Allen, J., and Kott, A. 2013a. "Resilience Metrics for Cyber Systems", Environment Systems & Decisions (33:4), Dec 2013 2014-02-19, pp 471-476.

Linkov, I., Senberg, D., Bates, M., Chang, D., Convertino, M., Allen, J., Flynn, S., and Seager, T. 2013b. "Measurable Resilience for Actionable Policy," Environmental Science & Technology (47:18), 2013/09/17, pp 10108-10110.

Nicholas, P. 2016. "Cybersecurity and Cyber-Resilience – Equally Important but Different".

North, J., and Pascoe, R. 2016. "Cyber Security and Resilience It's All About Governance", Governance Directions (68:3), p 146.

Putranti, I.R. 2015. "Developing of Cyber Resilience System of the International Trade Facilitations: Specific Reference Indonesia", Indonesia National Resilience Institute, p. 28.

Sarkar, A., Wingreen, S., and Cragg, P. 2013. "Organisational Is Resilience: A Pilot Study Using Q-Methodology", 24th Australasian Conference on Information Systems (ACIS): RMIT University, pp. 1-11.

Shapiro, S., Keys, B., Chhajer, A., Liu, Z., and Horner, D. 2016. "A Framework for Assessing Cyber Resilience", A Report for the World Economic Forum, p. 55.

Thebeau II, D., Reidy, B., Valerdi, R., Gudagi, A., Kurra, H., Al-Nashif, Y., Hariri, S., and Sheldon, F. 2014. "Improving Cyber Resiliency of Cloud Application Services by Applying Software Behavior Encryption (SBE)", Procedia Computer Science (28), pp 62-70.

Tran, H., Campos-Nanez, E., Fomin, P., and Wasek, J. 2016. "Cyber Resilience Recovery Model to Combat Zero-Day Malware Attacks", Computers & Security (61), pp 19-31.

Williams, P., and Manheke, R. 2010. "Small Business-a Cyber Resilience Vulnerability", 1st International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia.

World Economic Forum. 2012. "Partnering for Cyber Resilience, Risk and Responsibility in a Hyperconnected World - Principles and Guidelines."

Copyright