The least secure places in the universe? A Systematic Literature Review on Information Security Management in Higher Education

Ivano Bongiovanni[1,*]

1 Adam Smith Business School, University of Glasgow, Glasgow, UK

* Address correspondence to: Ivano Bongiovanni, Adam Smith Business School, East Quadrangle, Gilbert Scott Building, University of Glasgow, University Avenue, Glasgow G12 8QQ, UK; tel.: +44(0)141 330 1678; Ivano.Bongiovanni@glasgow.ac.uk

Abstract: Current research has demonstrated the progressively more strategic role that information security has in modern organisations. Higher education is no exception. The increasing number of security breaches experienced in recent years by higher education institutions epitomises the importance of confidentiality, integrity and availability of information in universities. To synthesise research in this field, this literature review systematically examines papers that have been published in the last thirteen years. The present review aims at expanding our understanding of the sub-topics, perspectives, methodologies, and trends that characterise this nascent field of investigation. Literature gaps are highlighted and an agenda for further work is proposed. First of its kind, this review concludes that information security management in higher education is a highly under-investigated topic. Areas for further research include information security culture; comparative studies on information security management in industries other than higher education; comparative studies across universities; and economics of information security management.

Keywords: information security management; cybersecurity; higher education; university; strategic information systems.

1 Introduction

In recent years, the diffusion of digital technologies has provided individuals, organisations, and society in general with entirely new opportunities. New possibilities for public and private organisations to collect, store and manage information and create new knowledge have emerged, to the point in which knowledge management has become an essential organisational component. The undeniable opportunities offered by the information age have come with new security requirements, which manifest in different forms: a landscape of constantly evolving IT best practices; new regulatory requirements in terms of data protection (e.g., the recent General Data Protection Regulation in Europe or the Notifiable Data Breaches scheme in Australia); and a scenario of emerging ethical issues. These requirements share a common origin: they are the technological, legal and ethical response to the increasing number of information security breaches experienced in recent years.

Information security revolves around the concepts of confidentiality, integrity, and availability of information (Whitson, 2003) and has expanded its importance and role in modern organisations: advisory firm Gartner predicts that worldwide security spending will reach around 124 billion USD in 2019, 22% more than 2017 and 10% more than 2018, with security services having the lion's share in IT security budgets (Gartner Inc., 2018). The growth in IT security spending is paralleled with the increasing importance of information security as the result of organisational decision-making and topics such as board of directors' role (Curry, 2017), information security culture (Beaver, 2015), and top management support (Bailey, Kaplan, & Rezek, 2014) are increasingly more debated in practitioners' literature. Despite the acknowledged role of security and privacy in information systems studies (Lowry, Dinev, & Willison, 2017), academic research falls behind, and topics such as managerial approach to information security (Phillips, 2013; Siponen, Adam Mahmood, & Pahnila, 2014; Soomro, Shah, & Ahmed, 2016), information security awareness (Parsons et al., 2017; Siponen et al., 2014), and the role of human factors (Jaeger, 2013; Vance, Lowry, & Eggett, 2013; Yeniman Yildirim, Akalp, Aytac, & Bayram, 2011) have only recently become subjects of scholarly investigation. Overall, in the literature, to complement the traditional, technical approach to information security, calls for further research on its organisational and managerial components have been multiplying (Parsons et al., 2017; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014; Phillips, 2013; Siponen et al., 2014; Soomro et al., 2016). The present review addresses such calls and explores the managerial aspects of information security, by focusing on a specific industry: Higher Education (HE).

2 Background

In 2004, Foster wrote that *'…related to computers, universities are among the least secure places in the universe.'* (2004, p. 1). Fifteen years later, penetration testing conducted by the Joint Information Systems Committee (JISC) in the UK has highlighted that through spear phishing there is a 100% chance of gaining access to a higher education institution's most valuable data within two hours (Chapman, 2019). Universities sit at one of the most *crowded* intersections of the digital economy: these open-by-design (Borgman, 2018; Chapman, 2019), decentralised, multi-stakeholder, transient platforms are traditionally associated with technology, research and innovation. Students, academics, staff and visitors regularly access universities' IT infrastructures to *consume* and produce data, in a multi-modal fashion: from personal mobile phones and smart-watches (*bring-your-own-device*, BYOD), through corporate laptops and tablets, to laboratory sensors and swipe access card systems, the data exchange among universities as organisations and their different categories of end-users is continuous.

As most modern organisations, universities are expanding their digital footprint, which increases their vulnerability to security breaches, and requires constant efforts in the field of security and privacy. At the same

time, the environment of HE seems to have a naturally idiosyncratic relationship with information security and its layered approach, rigid architecture, and centralised governance (Borgman, 2018; Hina & Dominic, 2016). As most universities do not have the resources necessary to provide centralised security services, partial outsourcing of information security is often the preferred solution (Chapman, 2019; Liu, Huang, & Lucas, 2017). This, on the one hand enables efficiency and more effective response to cyber-breaches, but on the other hand further enlarges academic institutions' digital footprint and requires adequate governance and contract management. Another issue is presented by the different degrees of knowledge of information security practices that categories of users have in universities, which makes training initiatives at best challenging (Lane, 2007). This latter aspect is exacerbated by the traditionally high turnover rate and by a generally complacent attitude towards information security (Noghondar, Marfurt, & Haemmerli, 2012). From an attacker's viewpoint, times when universities seemed not to own any attractive asset are long gone: from computational power (used, for example, to launch *distributed-denial-of-service* attacks or, more recently, to "mine" cryptocurrencies) through personal data (for example, students' social security numbers in the US), to intellectual property and some research data, universities are rapidly climbing hackers' interest lists (Roman, 2014).

As a result of these complex dynamics, the number of reported information security accidents in HE is growing throughout the world (Chapman, 2019), with several eminent cases making headlines in recent years (Table 1).

Date	Affected university/company	Country	Breach	Source
March 2019	Georgia Institute of Technology	US	An internal database was attacked and around 1.3M records were exposed.	(Prince & Sharpe, 2019)
February 2019	University of Washington	US	Almost 1M personal health records from the Medicine department were exposed due to internal human error	(Olenick, 2019)
June 2018	PageUp, recruitment provider for several Australian universities	Australia	Unusual activity detected around clients' data, indication of personal data of applicants being compromised by external attackers.	(Koziol, 2018)
June 2018	University of Utah	US	Theft of electronic equipment resulted in loss of personal data of 607 patients at the John A. Moran Eye Center.	(Donovan, 2018)
May 2018	University of Vermont	US	Security breach to NetID, the University's portal for online services, with potential impact on the personal data of 37,000 current and former faculty, staff and students	(Wallstin, 2018)
November 2017	University of East Anglia	UK	As a result of accidental use of a distribution list, the personal health information of a staff member was sent to 300 students in social sciences.	(SC Media, 2017)

Table 1 Recent information security breaches in universities (examples only; elaboration from Google)

Academic research on information security management in HE is still nascent (Marks, 2007; Okibo & Ochiche, 2014). At the same time, as demonstrated by prior research (Doherty, Anastasakis, & Fulford, 2009), information security in universities differs from other organisations, which renders information security

management in HE a research domain *per se*. To identify and analyse the state-of-the-art of this nascent field of research, the present paper proposes a systematic review of scholarly research on information security management in HE. This, to the best of our knowledge, is currently missing in the literature. The remainder of the paper is structured as follows: in the next section, the adopted methodology is introduced; then, the findings emerging from this review are presented; finally, conclusions are drawn and areas for further research recommended.

3 Methodology

The grounded theory approach proposed by Wolfswinkel, Furtmueller, and Wilderom (2013) was adopted, as inspired by prior work done by Webster and Watson (2002), and integrated by Pare, Tate, Johnstone, and Kitsiou (2016). The grounded theory approach allows the researcher to *"…advance the depth and breadth of an academic niche"* (Wolfswinkel et al., 2013, p. 46), as it inductively enables relevant concepts to surface from the literature. The adopted approach consisted of five phases (*define*, *search*, *select*, *analyse*, and *present*), complemented with a preliminary step, *develop* (Pare et al., 2016) to enhance systematicity and transparency.

First, a review plan around the topic of this study was *developed* and a set of research questions formulated to guide investigation (Booth, Sutton, & Papaioannou, 2016):

(1) What are the main topics explored in research on information security management in HE?
(2) How is information security management in HE investigated in the literature? When? Where? What sample, *foci*, formats and methodologies are adopted?
(3) Why is information security management in HE considered a relevant topic?
(4) What recommendations for a *research agenda* can be drawn from the literature?

Second; scope, field, sources and search terms were *defined*. The search was restricted to the following fields: social sciences, business and management, education, and computing science. In these, a database search was conducted, using keywords elaborated during the review planning phase, based on personal knowledge of the literature and review of key papers (Schatz & Bashroush, 2017). The wildcard character (*) was utilised for keyword completeness. Keywords were clustered in two groups, linked with the Boolean connector AND (Table 2).

Group	Keywords
Group 1	Information security management OR cybersecurity management OR cyber security management OR IT security management OR computer security management AND
Group 2	Universit* OR college* OR higher education

Table 2 Search groups and keywords

By restricting the search to specific fields and including the word 'management' in the keyword search, organisational and managerial issues were emphasised and a technical focus avoided. Due to the different search options in databases, minor adjustments were made to the search terms. Where possible, title, abstract and keywords were searched to ensure consistency with the search scope. To safeguard systematicity (Pare et al., 2016), all formats (journal articles, books, reports, etc.) were initially included in the search, regardless of sub-categories such as journal ranking, research methods or geographic region.

Third, relevant papers were *selected*, based on different criteria, identified to ensure relevance and rigour (Pare et al., 2016; Wolfswinkel et al., 2013). A first round of filtering focused on technical aspects: results were narrowed down by including only journal articles and conference papers, as representative of methodological rigour (Pare et al., 2016); documents in other languages than English were excluded; and so were duplicates across databases. A second round of filtering focused on metadata aspects: *false positives* were excluded where, for example, the words "university" or "college" recurred in the abstract only as authors'

affiliation details or for copyright reasons. A third round of filtering focused on substantial aspects: extensive analysis of abstracts led to the exclusion of documents that were *out of scope* (e.g., information security management was considered as a subject taught in HE degrees; research focus was only on university hospitals; or universities were utilised merely as a sample to conduct research on students' online behaviours). Two journal articles were also excluded as they appeared to have been blindly translated to English from another language, which created major issues with readability and comprehension. Lastly, one paper was excluded as almost identical to another one by the same authors, who have likely plagiarised their own work. After this refinement, a total of 40 documents were finally coded. Table 3 synthesises the sources utilised for the initial search.

Source	Search filters	Notes	Initial search
Scopus	Title, abstract, keywords	Multidisciplinary database search	62
Web of Science	Topic (title, abstract, author keywords and Keywords Plus®)	Multidisciplinary database search	29
ScienceDirect	Title, abstract, keywords	Multidisciplinary database search	13
ProQuest Academic	Abstract	Multidisciplinary database search	8
EBSCOHost	Abstract	Multidisciplinary database search	10
Emerald Insight Interdisciplinary	Title, abstract, keywords	Business Source Premier, EconLit, British Education Index, ERIC	0
Google Scholar	Keyword	Search engine	42
IEEE_Xplore	Abstract	Multidisciplinary database search	7
The ACM Guide to Computing Literature	Abstract	Multidisciplinary database search	20
TOTAL			191

Table 3 Search results

Fourth, *analysis* was performed by coding the text of the 40 papers (Wolfswinkel et al., 2013): using the research questions as a guide, broad categories and sub-categories of meaning were established, text attributed to each category and sub-category (open coding), logical connections drawn among the categories and sub-categories (axial coding), and the most relevant categories highlighted (selective coding).

Fifth, the results of the analysis were organised and presented in this paper.

4 Analysis of the results

The first research question of this literature review revolved around establishing what topics are mainly addressed by scholars investigating information security management in universities. Through open coding, a ranking of topics was established. Among the reviewed papers, 42% primarily focused on exploring *risk management frameworks and standards* utilised in universities to ensure information security management; on the other hand, *governance* of information security systems was addressed as the main topic by only 5% of the papers. Table 4 reports the ranking of topics and provides a description of sub-topics. Appendix 1 classifies the 40 reviewed papers by main topics.

Topic	Descriptor	Sub-topics	Frequency (papers)
Risk management frameworks and standards	Frameworks to manage information security as a risk entry, usually as derived from an organisational policy, potentially originating in turn from an international standard (e.g. ISO27001).	Framework formulation, implementation and assessment; information security management systems; risk and vulnerability assessment; etc.	17
Information security policies	As the conceptual basis for the risk management frameworks, information security policies define goals, operations (implementation) and performance (as compliance) of information security.	Formulation, implementation, and compliance; presence/absence of policies; fit with organisational strategy; adherence to international standards (ISO27001); etc.	5
Sociotechnical, holistic approach	Information security as encompassing both technical (e.g., IT architecture) and social components (e.g., training), with a view to extend it beyond IT departments.	End-users' role in information security; information security as 'everyone's business'; IT security as the product of organisational negotiations; human factors; etc.	5
Technical solutions	Engineering, solution-oriented perspective on information security, with a broad range of sub-topics mainly addressing effectiveness of cyber-defences.	Security threats; security layers and controls; web applications; campus network protection; etc.	4
Cyber-behaviours	End-point vulnerability as mainly determined by human factors (e.g., intentions, perceptions).	Life-style routines; protection motivation; outcome expectations; social networking habits; etc.	4
Culture and awareness	As a component of organisational culture, information security culture is determined, among others, by employees' degree of awareness, top management support, and end-users' cyber-behaviours.	Information security training; cultural approach to information security in the youth.	3
Governance	How organisations decide to plan for, and manage, their information security.	Managed security services; outsourcing; decentralisation.	2

Table 4 Ranking of the main topics in the papers, descriptors and sub-topics

A total of 149 keywords were produced by 36 papers (4 papers did not include any). The keywords were "cleaned", where necessary, aggregated (e.g., singular and plural forms of the same concept; synonyms; etc.), and then analysed. Consistency with the main topics was highlighted by focusing on the most recurrent keywords: *information security* (14 papers), *information security management system* (6), *information security policy* (6), *information security management* (5), *higher education* (4), *information systems security* (4), and *security threat* (4). Interestingly, *cybersecurity breach* was only reported as a keyword by 3 papers. The significant variety of sub-topics addressed in the papers was demonstrated by the number of unique keywords, 74.

The second research question explored *year*, *location*, *sample*, *focus*, *format*, and *methodologies* of the 40 papers in the sample. Figure 1 shows how the number of academic publications on information security management in universities, though still quite low, is growing in recent years, with 21 publications in the period 2014-2017 compared to four in the years 2005-2008.

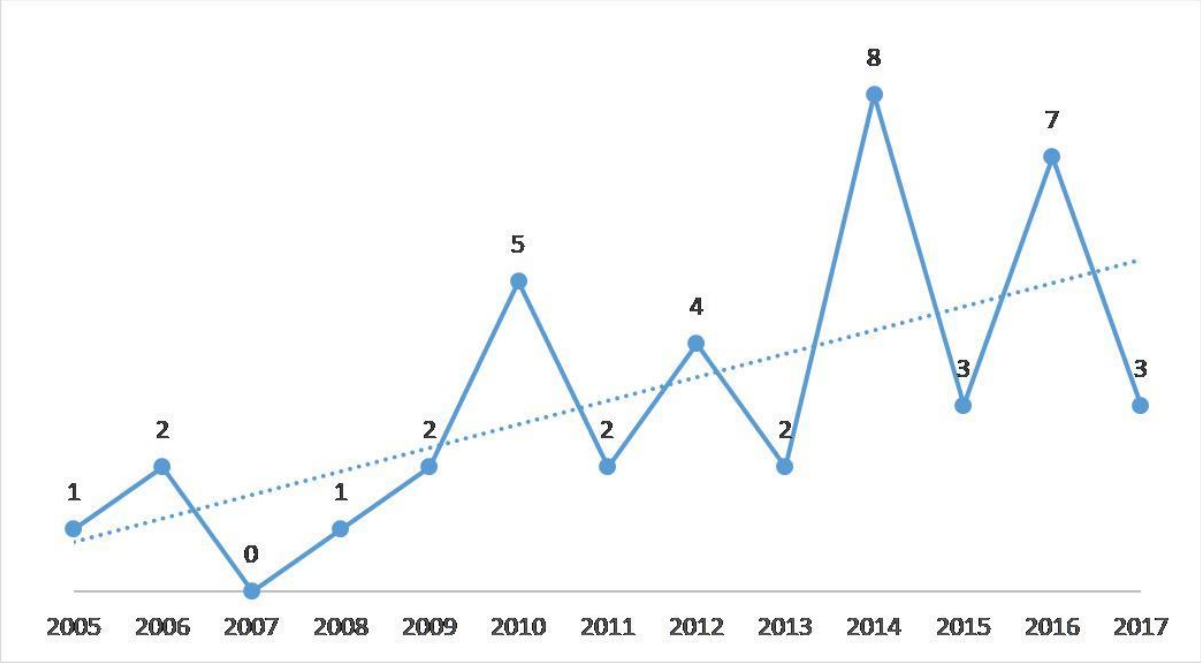

Fig. 1 Number of publications per year with trend

The geography of such studies indicates significant diversity, with 21 unique countries out of 40 papers. The United States were the location of 6 studies, followed by Malaysia and China with 4 and Indonesia with three. Two studies were multi-country (US, UK, Australia, Canada, New Zealand, Hong Kong, and Ireland) and two did not refer to a specific location. Eleven countries had one study conducted. Adopted sample populations differed greatly across the 40 papers and the following categories were identified: end-users (e.g., 273 students in a communication major), groups of end-users (e.g., 72 IT employees across 6 engineering schools; 152 IT and administrative staff across three universities), research group, department (e.g., medical college), groups of departments (e.g., 11 academic hospitals), university, groups of universities (e.g., 3 universities in one country), and groups of HE institutions (e.g., 505 higher education institutions in one country). More specifically, the majority of papers (19) focused on a university-wide study (e.g., to assess the effectiveness of the information security management system implemented across the whole university); 6 papers focused on students (e.g., to understand the motivations behind their unsafe cyber-behaviours); 4 on IT applications (e.g., to test the security of an *Examination Paper Preparation Process*); another 4 on the IT department of a university; etc. In terms of format, the 40 papers were almost equally distributed between journal articles (18) and conference papers/proceedings (22).

Figure 2 represents the research methodologies mainly utilised by the authors of the explored papers.

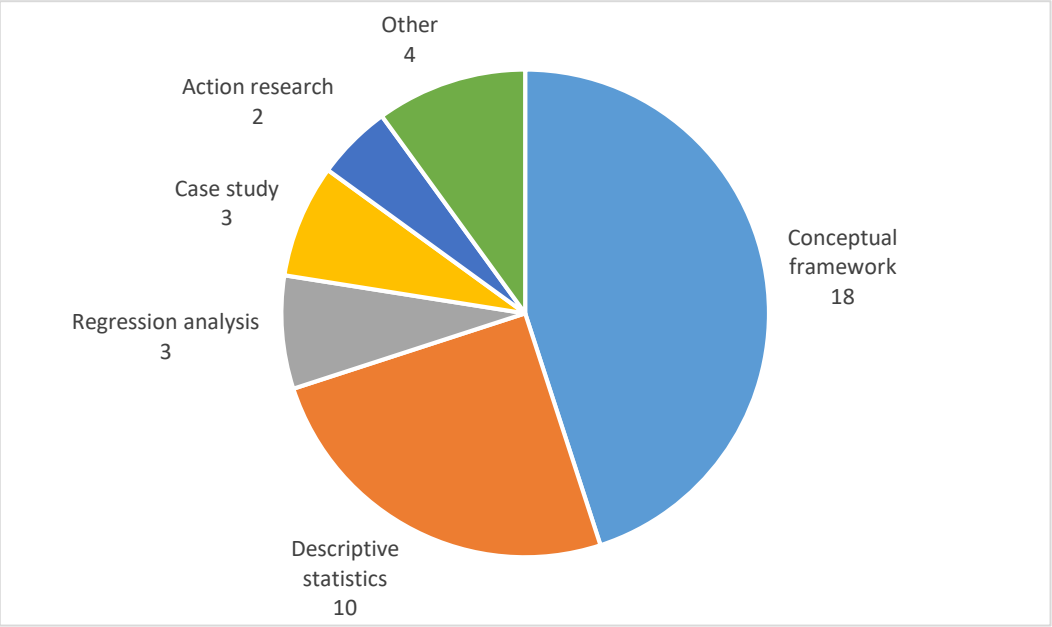

Fig. 2 Research methodologies adopted in the sample

Conceptual frameworks were by far the most represented in the sample, with 18 papers proposing their version of "a most effective" information security management system or policy. These frameworks were mainly elaborated from literature reviews and document analysis (e.g., ISO27001) and around half of them were not quantitatively tested. Besides conceptual frameworks, *descriptive statistics* were utilised in 10 papers to illustrate phenomena such as information security challenges in universities, perceptions of safe online behaviours, implementation of practical information security guidelines, etc. On the other hand, *regression analysis* was adopted by only three papers. Among the least utilised research methodologies (indicated in Figure 2 as "other"), *inferential statistics (structural equation modelling)*, *inferential statistics (factor analysis)*, *cross-functional study*, and a *mixed descriptive statistics-qualitative analysis*, with one paper each. Of the 40 pieces of research in the sample, 20 analysed *primary data* only (from surveys, questionnaires, interviews, lab testing and observation), 7 *secondary data* only (from document analysis, databases, literature and regulation review), and four *mixed primary and secondary data*. The remaining 9 pieces of research proposed conceptual frameworks but did not test them.

The third research question aimed at understanding why information security management is a topic worth exploring in universities. Open coding revolved around examining if, and how, authors justified exploring HE, rather than, for instance, another industry. Findings highlighted how most papers (11) provided little to no justification for investigating the topic of information security management in HE. Ten papers explicitly described universities as open, multi-modal platforms, whose organisational complexity has the potential to increase vulnerability to information security breaches. Two papers focused on universities as knowledge-intensive organisations for which protection of knowledge has a strategic value. The remaining 17 papers explored the specificity of information security management in HE by justifying its relevance based on these arguments:

- Universities host many diverse systems; are a fertile ground for IT exploration; host future innovators and leaders, who are the baseline for information security awareness for future generations; and are eclectic environments with different cultures and technologies, that need to be balanced with business and corporate requirements;

- Universities produce legal documents (e.g., degree certificates), whose confidentiality, integrity and availability must be protected;
- IT technologies, and a BYOD mind set, have wide-spread diffusion in universities;
- There is a growing number of security breaches in universities;
- Universities are open innovation platforms and public organisations;
- Due to the weakness of information security technology and its increasing attractiveness for malevolent individuals, websites of universities and colleges have become an important target for hackers;
- Traditionally universities are deemed to be insecure from an IT standpoint (for example, their websites);
- Universities are experiencing growing enrolments, and becoming as a result more vulnerable as organisations;
- Universities hold extensive amount of hard-copy materials that need protection from security threats.

Several authors had a specific focus on students as end-users of the university networks, with investigation of social networking behaviours, of vulnerability to *dangerous webpages*, and of vulnerability as an indicator for information security management's effectiveness.

The fourth research question synthesised recommendations for further research in the field of information security management in universities. In general, the reviewed papers contained little to no explicit recommendation for future research in the field. Among the studies that did indicate areas for further exploration (17), researchers proposed to utilise universities as a proxy for further investigating information security in public organisations, or as a benchmark to do so in private organisations. Others suggested to further investigate an information security management system tailored to the university environment, to explore the alignment existing between information security policies and universities' strategic documents, or to better understand how an acceptable use policy could apply to a university. Similarly, other papers raised attention around further benchmarking information security management across universities. Human factor analysis was another area for future investigation, in particular in the fields of unintentional data leakage, end-users' perceptions of cyber-behaviours, the role of cyber-routines in the offender-offended dynamic, and intentions to avoid malware when in a work-at-work and a work-at-home situation.

5 Discussion

Unsurprisingly, the present literature review indicates that the explored papers focused on the organisational and managerial aspects of information security. Technical components (e.g., universities' security architecture) were mainly utilised to draw organisational conclusions, in terms of ensuring information security in the whole university system. This is consistent with calls in the literature for an enhanced role of a managerial, holistic approach to information security, not only in HE (Soomro et al., 2016). It is therefore natural for topics such as risk management frameworks, organisational security policies and sociotechnical aspects of information security to emerge as the predominant ones. On the contrary, it is surprising to notice how information security culture and awareness were the main focus for only three papers, given the growing interest in these topics in other contexts and industries (Parsons et al., 2017; Singh, Picot, Kranz, Gupta, & Ojha, 2013; Siponen et al., 2014). To explain this, we can hypothesise that the potential number of information security "cultures" existing in universities (e.g., a student's perception of information security may completely differ from a researcher's, or an administrative staff member's) discourages researchers from undertaking the challenging task of defining "one culture". This, in hindsight, renders this research topic more appealing from a scientific viewpoint.

International standards and shared best practices are another recurrent theme in the explored papers. In a research domain that is not "natural" for scholars in business and management, as more closely related to computing science and engineering (Kotulic & Clark, 2004), researchers investigate information security starting from agreed practices and regulations to then venture out to more untapped topics such as human factors, perceptions, and behaviours.

The present literature review demonstrates how information security management in HE is a new topic of interest, with most publications emerging in recent years. The presence of numerous studies (9) in which the

proposed conceptual frameworks are not empirically tested further supports the notion of a nascent field of research (Edmondson & Mcmanus, 2007), in which theories have not been fully developed yet, and quantitative methods are more hardly conceivable. From a geographical perspective, besides a "traditional" hegemony by the US and a globally diffused interest in the topic, it is worth noting that South East Asian researchers have been consistently publishing, with China, Malaysia and Indonesia combining 11 papers. The difficulties associated with conducting research in information security (Kotulic & Clark, 2004), a domain in which researchers traditionally experience barriers in information sharing, may explain the fact that only two studies were multi-country. Further to this, both such studies utilised only secondary data (e.g., open access databases). Findings of this review underline that several papers did not provide a detailed justification as for the specificity of information security as managed in HE. Several pieces of research appeared to have incidentally utilised universities as units of analysis, for various practical reasons; above all, ease of access by researchers. Those studies that did provide arguments for HE's specificity, confirmed prior research on this subject (Borgman, 2018; Lane, 2007; Luker & Petersen, 2003; Marks, 2007; Rezgui & Marks, 2008): universities have a multi-modal, open-by-design architecture that naturally facilitates information exchange; the presence of numerous connected devices, together with the co-existence of different security cultures, across organisational roles and countries (e.g., students, researchers, staff members) and a tendency to outsource security controls renders universities more susceptible to internal threats (e.g. complacency); lastly, the expanding value of data as a currency (e.g., IP, interview transcripts and personal data), coupled with the innovative mind-set fostered by academic institutions, makes them an interesting target for external attackers.

A final consideration on areas for further research needs to account for the quality of the studies reviewed in the present paper: a number of them had major limitations in terms of methodological rigour, and practical and theoretical contributions. This can in part be explained by the different research backgrounds of the authors (management, education, computing science, to name a few), which entails different research methodologies and approaches. As a result, we can conclude that major gaps exist in literature on information security management in HE. The present review recommends further work in four areas: 1) information security culture, to understand what different degrees of awareness students, researchers, visitors and staff members have, and to assess and improve information security training; 2) comparative studies on information security management in HE and other industries, traditionally taken as best practices (e.g., banking and aviation); 3) comparative studies across universities, to facilitate the diffusion of virtuous examples; and 4) economics of information security management, to support top management with budgeting decisions and resource allocation. From a practical viewpoint, research in the aforementioned avenues would greatly benefit from engagement with practitioners (e.g., IT security managers, Chief Information Security Officers), as well as end-users. As an example, the author of the present paper is currently exploring options for co-designing information security training courses with, and for, the different categories of end-users in universities.

6 Conclusions

This literature review is, to the best of our knowledge, the first attempt to systematise the existing contributions of scholarly investigation to the field of information security management, as applied to higher education institutions. By adopting a grounded theory approach, anchored in work that utilised a method intended to enhance systematicity and transparency (Pare et al., 2016), this examination has produced theoretical contributions in several ways. First and foremost, it has highlighted the complexity of universities, with regards to the practices they implement when dealing with the confidentiality, integrity and accessibility of the information they hold at any given time. It has done so by identifying seven main topics (and numerous sub-topics) addressed in the literature, ranging from the adoption of risk management frameworks and standards, through technical solutions to cyber-related problems, to governance systems implemented to effectively manage information security. Also, this paper has documented that research in this field is still *nascent*, as most works were published in or after 2014. This demonstrates a growing interest, and the need to increase research efforts in this area; this is also witnessed by the number of conceptual papers and the lack of quantitative studies in the sample, and by the fact that the majority of the reviewed articles have not provided specific reasons for investigating information security management in universities and research centres. As a final theoretical contribution, this paper has summarised areas for further research in this field including, for example, information security culture and benchmark studies between higher education and other industries. Despite its primarily theoretical nature, a literature review can offer some practical contributions too, and this paper is no

exception. IT executives and information security professionals in universities can benefit from its holistic and synthetic approach and expand their understanding of the status quo of research on information security management. Similarly, security professionals with limited experience in higher education can draw from this review an outline of the very nature of higher education, whose open architecture, organisational cultures and multitude of users constitute a challenge from a security and privacy standpoint.

References

Abdelwahed, A. S., Mahmoud, A. Y., & Bdair, R. A. (2016). Information Security Policies and their Relationship with the Effectiveness of the Management Information Systems of Major Palestinian Universities in the Gaza Strip. *International Journal of Information Science and Management (IJISM), 15*(1).

Arafat, J., Daiyan, G. M., & Waliullah, M. (2012). Emergence of Robust Information Security Management Structure around the world wide Higher Education Institutions: a Multifaceted Security Solution. *International Journal of Computer Science Issues (IJCSI), 9*(4), 206.

Bailey, T., Kaplan, J., & Rezek, C. (2014). Why senior leaders are the front line against cyberattacks. Retrieved 25 June, 2018, from https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/why-senior-leaders-are-the-front-line-against-cyberattacks

Beaver, K. (2015). The Importance of a Security Culture Across the Organization. Retrieved 25 June, 2018, from https://securityintelligence.com/the-importance-of-a-security-culture-across-the-organization/

Bhilare, D. S., Ramani, A. K., & Tanwani, S. K. (2009, 11-14 October 2009). *Protecting intellectual property and sensitive information in academic campuses from trusted insiders: leveraging active directory.* Paper presented at the 37th annual ACM SIGUCCS fall conference: communication and collaboration, St. Louis, Missouri, USA.

Booth, A., Sutton, A., & Papaioannou, D. (2016). *Systematic approaches to a successful literature review* (Second ed.). London: Sage Publications Ltd.

Borgman, C. L. (2018). Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier. *arXiv preprint arXiv:1802.02953*.

Candiwan, Sari, P. K., & Nurshabrina, N. (2016, 9-11 June). *Assessment of information security management on Indonesian higher education institutions.* Paper presented at the 2nd International Conference on Communication and Computer Engineering, ICOCOE 2015, Phuket, Thailand.

Chapman, J. (2019). How safe is your data? Cyber-security in higher education. In Higher Education Policy Institute (Ed.), *HEPI Policy Note* (Vol. 12, pp. 1-6). Oxford, UK: Higher Education Policy Institute,.

Cheung, S. K. S. (2014, 13-15 June). *Information security management for higher education institutions.* Paper presented at the 1st Euro-China Conference on Intelligent Data Analysis and Applications, ECC 2014, Shenzen, China.

Choi, K. S., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior, 73*, 394-402. doi: 10.1016/j.chb.2017.03.061

Curry, S. (2017). Boards Should Take Responsibility for Cybersecurity. Here's How to Do It. *Harvard Business Review*. https://hbr.org/2017/11/boards-should-take-responsibility-for-cybersecurity-heres-how-to-do-it

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers and Security, 48*, 281-297. doi: 10.1016/j.cose.2014.11.002

Das, S., Mukhopadhyay, A., & Bhasker, B. (2013). Today's action is better than tomorrow's cure - Evaluating information security at a premier Indian business school. *Journal of Cases on Information Technology, 15*(3), 1-22. doi: DOI: 10.4018/jcit.2013070101

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT, 29*(6), 449-457. doi: 10.1016/j.ijinfomgt.2009.05.003

Doherty, N. F., Anastasakis, L., & Fulford, H. (2011). Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy. *INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT, 31*(3), 201-209. doi: https://doi.org/10.1016/j.ijinfomgt.2010.06.001

Donovan, F. (2018). Dignity Health Data Breach Affects 55.9K Patients. Retrieved 25 June, 2018, from https://healthitsecurity.com/news/dignity-health-data-breach-affects-55.9k-patients

Edmondson, A. C., & Mcmanus, S. E. (2007). Methodological fit in management field research. *Academy of Management Review, 32*(4), 1155-1179. doi: 10.5465/amr.2007.26586086

Foster, A. L. (2004). Insecure and Unaware. An analysis of campus networks reveals gaps in security. Retrieved 25 June, 2018, from https://www.chronicle.com/article/InsecureUnaware/11671

Gartner Inc. (2018). Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. Retrieved 29 November, 2018, from

https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

Hedström, K., Dhillon, G., & Karlsson, F. (2010, 20-23 September). *Using Actor Network Theory to understand information security management.* Paper presented at the 25th IFIP TC-11 International Information Security Conference, SEC 2010, Brisbane, Australia.

Hina, S., & Dominic, D. D. (2016, 15-17 August 2016). *Information security policies: Investigation of compliance in universities.* Paper presented at the 3rd International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur.

Hommel, W., Metzger, S., & Steinke, M. (2015). Information Security Risk Management in Higher Education Institutions: From Processes to Operationalization. *EUNIS Journal of Higher Education IT, 2015*(3).

Hussein, R., & Lambensa, F. (2010, 23-24 June). *An empirical investigation on information security behavior: A case of a Malaysian public university.* Paper presented at the 14th International Business Information Management Association Conference, IBIMA 2010, Istanbul, Turkey.

Ismail, W., Norwawi, N. M., & Saadan, K. (2014, 12-15 August). *The Challenges in Adopting Information Security Management System for University Hospitals in Malaysia.* Paper presented at the Knowledge Management International Conference (KMICe) 2014, Kuala Lumpur, Malaysia.

Ismail, W. H., & Widyarto, S. (2016, 21-22 April). *A Formulation and Development Process of Information Security Policy in Higher Education.* Paper presented at the 1st International Conference on Engineering Technology and Applied Sciences Afyonkarahisar, Turkey.

Ismail, Z., Masrom, M., Sidek, Z. M., & Saaid, I. (2010, 25 March). *Bridging Information Security Framework for Higher Learning Institutions of Malaysia.* Paper presented at the International Conference on Information Management and Evaluation, Cape Town, South Africa.

Itradat, A., Sultan, S., Al-Junaidi, M., Qaffaf, R., Mashal, F., & Daas, F. (2014). Developing an ISO27001 information security management system for an educational institute: Hashemite university as a case study. *Jordan Journal of Mechanical and Industrial Engineering, 8*(2), 102-118.

Jaeger, J. (2013). Human error, not hackers, cause most data breaches. Retrieved 25 June, 2018, from https://www.complianceweek.com/news/news-article/human-error-not-hackers-cause-most-data-breaches#.WzDycadKiUk

Joshi, C., & Singh, U. K. (2017). Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications, 35*, 128-137. doi: 10.1016/j.jisa.2017.06.006

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*(5), 597-607. doi: 10.1016/j.im.2003.08.001

Koziol, M. (2018). Major universities hit by data breach affecting thousands of job applicants at top firms. Retrieved 25 June, 2018, from https://www.smh.com.au/politics/federal/major-universities-hit-by-data-breach-affecting-thousands-of-job-applicants-at-top-firms-20180608-p4zkd9.html

Lane, T. (2007). *Information security management in Australian Universities: An exploratory analysis.* Queensland University of Technology.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour and Information Technology, 27*(5), 445-454. doi: 10.1080/01449290600879344

Lewis, N., Campbell, M. J., & Baskin, C. R. (2015). Information security for compliance with select agent regulations. *Health security, 13*(3), 207-218. doi: 10.1089/hs.2014.0090

Li, X. L. (2016, 3-4 September). *The Design of Information Security Management System in College.* Paper presented at the International Conference on Education & Educational Research and Environmental Studies (EERES 2016), Hong Kong.

Liu, C.-W., Huang, P., & Lucas, H. (2017, 10-13 December). *IT Centralization, Security Outsourcing, and Cybersecurity Breaches: Evidence from the US Higher Education.* Paper presented at the International Conference on Information Systems ICIS 2017, Seoul, South Korea.

Loser, K. U., Nolte, A., Herrmann, T., & Te Neues, H. (2011, 8 September). *Information security management systems and socio-technical walkthroughs.* Paper presented at the 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST), Milan, Italy.

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda. *European Journal of Information Systems, 26*(6), 546-563. doi: 10.1057/s41303-017-0066-x

Luker, M. A., & Petersen, R. J. (2003). *Computer and network security in higher education* (Vol. no. 8). San Francisco, CA: Jossey-Bass.

Maidabino, A. A., & Zainab, A. N. (2012). A holistic approach to collection security implementation in university libraries. *Library Collections, Acquisitions, and Technical Services, 36*(3), 107-120. doi: https://doi.org/10.1016/j.lcats.2012.05.004

Marks, A. A. (2007). *Exploring universities' information systems security awareness in a changing higher education environment: a comparative case study research.* University of Salford.

Massacci, F., Prest, M., & Zannone, N. (2005). Using a security requirements engineering methodology in practice: The compliance with the Italian data protection legislation. *Computer Standards and Interfaces, 27*(5), 445-455. doi: 10.1016/j.csi.2005.01.003

May, L., & Lane, T. (2006). A Model for Improving e-Security in Australian Universities. *Journal of Theoretical & Applied Electronic Commerce Research, 1*(2), 90-96.

Mogale, M., Gerber, M., Carroll, M., & Von Solms, R. (2014, 13-14 August). *Information security assurance model (ISAM) for an examination paper preparation process.* Paper presented at the 2014 Information Security for South Africa ISSA, Johannesburg, South Africa.

Ngoqo, B., & Flowerday, S. V. (2014, 17-19 November). *Student information security behavioural intent: Assessing the actions and intentions of students in a developmental university.* Paper presented at the 7th International Conference of Education, Research and Innovation ICERI 2014, Seville, Spain.

Nie, J., & Dai, X. L. (2017, 16-19 December). *On the Information Security Issue in the Information Construction process of colleges and universities.* Paper presented at the 12th International Conference on Computational Intelligence and Security (CIS), Wuxi, China.

Noghondar, E. R., Marfurt, K., & Haemmerli, B. (2012, 9-13 May). *The human aspect in data leakage prevention in academia.* Paper presented at the 35th International Spring Seminar on Electronics Technology ISSE 2012, Bad Aussee, Austria.

North, M. M., George, R., & North, S. M. (2006, 10-12 March). *Computer Security and ethics awareness in university environments: A challenge for management of information systems.* Paper presented at the 44th ACM Southeast Regional Conference, Melbourne, Florida.

Okibo, B. W., & Ochiche, O. B. (2014). Challenges Facing Information Systems Security Management in Higher Learning Institutions: A Case Study of the Catholic University of Eastern Africa-Kenya. *International Journal of Management Excellence, 3*(1), 336-349.

Olenick, D. (2019). Misconfigured database exposes 974,000 University of Washington Medicine patients. Retrieved 16 April, 2019, from https://www.scmagazine.com/home/security-news/data-breach/misconfigured-database-exposes-974000-university-of-washington-medicine-patients/

Paiziaihemaiti, A., & Arxiden, A. (2016, 11-12 June). *Research on Network Information Security Analysis and Prevention Strategies of Campus Network in Xinjiang Uygur Medical College.* Paper presented at the 6th International Conference on Machinery, Materials, Environment, Biotechnology and Computer (MMBEC 2016), Tianjin, China.

Pare, G., Tate, M., Johnstone, D., & Kitsiou, S. (2016). Contextualizing the twin concepts of systematicity and transparency in information systems literature reviews. *European Journal of Information Systems, 25*(6), 493-508. doi: 10.1057/s4I303-016-0020-3

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40-51. doi: 10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176. doi: 10.1016/j.cose.2013.12.003

Phillips, B. (2013). Information Technology Management Practice: Impacts upon Effectiveness. *Journal of Organizational and End User Computing (JOEUC), 25*(4), 50-74. doi: 10.4018/joeuc.2013100103

Prince, C., & Sharpe, J. (2019). Data breach exposes up to 1.3M Georgia Tech faculty, students. Retrieved 16 April, 2019, from https://www.ajc.com/news/breaking-news/breaking-data-breach-exposes-georgia-tech-faculty-students/zAUUNWy5hoHQ8bNvMxcsWL/

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*(7), 241-253. doi: 10.1016/j.cose.2008.07.008

Roman, J. (2014). University Breaches: A Continuing Trend. Retrieved 25 June, 2018, from https://www.databreachtoday.asia/university-breaches-continuing-trend-a-6660

Romero, M. B. D., & Haddad, H. M. (2010, 12-14 April). *Asset assessment in web applications.* Paper presented at the 7th International Conference on Information Technology: New Generations (ITNG 2010), Las Vegas, Nevada.

Sari, P. K. (2012, 4-6 July). *A concept of information security management for higher education.* Paper presented at the 3rd International Conference on Technology and Operation Management, Bandung, Indonesia.

Sari, P. K., Nurshabrina, N., & Candiwan. (2016, 26-27 April). *Factor analysis on information security management in higher education institutions.* Paper presented at the 4th International Conference on Cyber and IT Service Management (CITSM), Bandung, Indonesia.

SC Media. (2017). UK University fails to learn - UEA, a data breach repeat offender. Retrieved 25 June, 2018, from https://www.scmagazineuk.com/uk-university-fails-to-learn--uea-a-data-breach-repeat-offender/article/706760/

Schatz, D., & Bashroush, R. (2017). Economic valuation for information security investment: a systematic literature review. *Information Systems Frontiers, 19*(5), 1205-1228. doi: 10.1007/s10796-016-9648-8

Silva, M. M., de Gusmão, A. P. H., Poleto, T., Silva, L. C. e., & Costa, A. P. C. S. (2014). A multidimensional approach to information security risk management using FMEA and fuzzy theory. *INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT, 34*(6), 733-740. doi: https://doi.org/10.1016/j.ijinfomgt.2014.07.005

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. *Global Journal of Flexible Systems Management, 14*(4), 225-239. doi: 10.1007/s40171-013-0047-4

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224. doi: https://doi.org/10.1016/j.im.2013.08.006

Soomro, Z., Shah, M., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT, 36*(2), 215-225. doi: 10.1016/j.ijinfomgt.2015.11.009

Tavakoli, N., Ehteshami, A., Hassanzadeh, A., & Amini, F. (2014). Information Security Management in Isfahan University of Medical Sciences' Academic Hospitals in 2014. *International Journal of Health System and Disaster Management, 2*(3), 175.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using Accountability to Reduce Access Policy Violations in Information Systems. *Journal of Management Information Systems, 29*(4), 263-290. doi: 10.2753/mis0742-1222290410

Wallstin, B. (2018). UVM warns faculty, students of potential breach of personal data. Retrieved 25 June, 2018, from https://www.mychamplainvalley.com/news/local-news/uvm-warns-faculty-students-of-potential-breach-of-personal-data/1198682851

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly, 26*(2), xiii-xxiii.

Whitson, G. (2003). Computer security: theory, process and management. *Journal of computing sciences in colleges, 18*(6), 57-66.

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. M. (2013). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems, 22*(1), 45-55. doi: 10.1057/ejis.2011.51

Yamanoue, T., Furuya, T., Shimozono, K., Masuya, M., Oda, K., & Mori, K. (2013, 3-8 November). *Enhancing information security of a university using computer ethics video clips, managed security service and an information security management system.* Paper presented at the 41st annual ACM SIGUCCS Conference on User services, Chicago, IL.

Yeniman Yildirim, E., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT, 31*(4), 360-365. doi: 10.1016/j.ijinfomgt.2010.10.006

Zhu, J., Xu, B., Jiang, B., & Chen, W. (2010, 22-23 May). *Identifying harmful web pages in laboratory information security management.* Paper presented at the 2nd International Workshop on Intelligent Systems and Applications ISA 2010, Wuhan, China.

Appendix 1: Reviewed papers classified by main topics (in alphabetical order)

Risk management frameworks and standards

(Arafat, Daiyan, & Waliullah, 2012)

(Candiwan, Sari, & Nurshabrina, 2016)

(Cheung, 2014)

(Das, Mukhopadhyay, & Bhasker, 2013)

(Hommel, Metzger, & Steinke, 2015)

(W. Ismail, Norwawi, & Saadan, 2014)

(Z. Ismail, Masrom, Sidek, & Saaid, 2010)

(Itradat et al., 2014)

(Joshi & Singh, 2017)

(Lewis, Campbell, & Baskin, 2015)

(Li, 2016)

(Maidabino & Zainab, 2012)

(Massacci, Prest, & Zannone, 2005)

(May & Lane, 2006)

(Mogale, Gerber, Carroll, & Von Solms, 2014)

(Sari, 2012)

(Silva, de Gusmão, Poleto, Silva, & Costa, 2014)

Policies: formulation, implementation, compliance

(Abdelwahed, Mahmoud, & Bdair, 2016)

(Doherty, Anastasakis, & Fulford, 2011)

(Doherty et al., 2009)

(W. H. Ismail & Widyarto, 2016)

(Tavakoli, Ehteshami, Hassanzadeh, & Amini, 2014)

Sociotechnical, holistic approach

(Hedström, Dhillon, & Karlsson, 2010)

(Loser, Nolte, Herrmann, & Te Neues, 2011)

(Noghondar et al., 2012)

(Okibo & Ochiche, 2014)

(Sari, Nurshabrina, & Candiwan, 2016)

Technical solutions

(Bhilare, Ramani, & Tanwani, 2009)

(Paiziaihemaiti & Arxiden, 2016)

(Romero & Haddad, 2010)

(Zhu, Xu, Jiang, & Chen, 2010)

Cyber-behaviours

(Dang-Pham & Pittayachawan, 2015)

(Choi & Lee, 2017)

(Hussein & Lambensa, 2010)

(Lee, Larose, & Rifon, 2008)

Culture and awareness

(Ngoqo & Flowerday, 2014)

(North, George, & North, 2006)

(Yamanoue et al., 2013)

Governance

(Liu et al., 2017)

(Nie & Dai, 2017)