Securing Intellectual Capital: An Exploratory Study in Australian Universities

Ivano Bongiovanni (*Adam Smith Business School, University of Glasgow, Glasgow, UK*)

Karen Renaud (*Division of Cyber Security, Abertay University, Dundee, UK and Rhodes University, Grahamstown, South Africa*)

George Cairns (*QUT Business, Brisbane, Australia*)

Structured Abstract:

Purpose – To investigate the links between IC and the protection of data, information and knowledge in universities, as a special kind of organization with unique knowledge-related challenges.

Design/methodology/approach – We gathered insights from existing IC-related research publications to delineate key foundational aspects of IC, and proposed links to traditional information security that impact the protection of IC. We conducted interviews with key stakeholders in Australian universities in order to test these links.

Findings – Our investigation revealed two kinds of embeddedness characterising the organizational fabric of universities, vertical and horizontal, and with emphasis on the connection between these and IC-related protection within the institutions.

Research implications – There is a need to acknowledge the different roles played by actors within the university, and the relevance of information security for IC protection.

Practical implications – Framing information security as an IC-related issue can help IT security managers communicate more effectively with executives in higher education institutions.

Originality/value – This is one of the first studies to explore the connections between the traditional data, information and knowledge security and the three core components of IC.

Keywords: Intellectual capital, Data security, Information security, Knowledge security, Cybersecurity, Higher education, University.

Paper type Research paper

Introduction

Intellectual Capital (IC) is the stock of knowledge held by an organization (Dierickx and Cool, 1989), and made up of three components: human (HC) (the product of individual intellectual action, such as individual tacit knowledge), structural capital (SC) (organizational processes, systems and routines that structure intellectual assets into group property), and relational or customer capital (RC) (understanding of ex-firm intangibles, such as customer needs) (Bontis, 1998). Knowledge is at the core of IC (Stewart, 1998) with organizations being considered "repositories and coordinators of intellect" (Quinn, 1992, p. 241), this being intrinsically linked to organizations' economic wealth and value creation (Paloma Sánchez and Elena, 2006). There is a growing interest (in both research and practice) into the role of IC in educational institutions (Bisogno *et al.*, 2018) and particularly in universities (Paloma Sánchez *et al.*, 2009), who consider IC management crucially important (Secundo *et al.*, 2015).

In this paper, we argue that universities are exposed to significant challenges in terms of the ways in which they secure their IC-related data, information and knowledge. Research shows that, in universities, this is shaped by their existing structural assets, whose contribution to the value creation process is significant (Di Berardino and Corsi, 2018). In particular, we investigate how universities secure the knowledge they produce, transmit

and disseminate, and explore links to organization-held data and information, and the security thereof. To achieve this, our investigation focuses on data and information security management in universities and research centres. Our findings unpack IC's three foundational components and expand our understanding of how these are influenced by data and information security practices in 10 universities and one major research centre in Australia.

Following an overview of the theoretical background, we outline our research design. We then present and discuss our findings within the context of existing literature and practices, before concluding our paper and suggesting further research directions.

Our contribution to the field of IC includes the following:

- We explore the particular nature of IC in higher education institutions, considering whether it extends beyond its traditional tripartite structure (HC, SC, and RC);
- We unpack the relationships between IC's instantiations, namely data, information and knowledge; especially as this applies to their protection within universities;
- We conclude by providing security managers in universities with an original lens to decode and communicate, to university management, the potential impact that poor information security could have on IC.

Review of the literature

Intellectual Capital, Knowledge Management and Information Security

In the knowledge economy, public and private organizations are required to increase their emphasis on managing the knowledge they produce (Bontis, 1998). Effective knowledge management systems increase organizations' competitive advantage and assure their very survival in times of crisis (Nahapiet and Ghoshal, 1998). In the light of these trends, the

concept of intellectual capital (IC) has emerged as an area in which effective investments have the potential to yield a competitive edge. Traditionally neglected in management studies, IC is strictly associated with the concept of value creation, whereby a set of organizational, intangible assets has the intrinsic potential to create wealth, or add value.

Researchers have conceptualized IC in different ways. Stewart (1998) aligns IC with knowledge, information, data and Intellectual Property (IP). Nahapiet and Ghoshal (1998) describe IC as knowledge and knowing capability whereas Dierickx & Cool (1989) refer to IC as a "stock of knowledge". Asiaei and Jusoh (2015) mention IC's link to know-how and knowledge of manpower, databases, information technology, operating processes, customer relationships, brand, trust and cultures. Researchers and practitioners alike have also started identifying ways to operationalise IC, to conceive it as a construct, with the purpose of measuring, assessing and managing it.

Bontis (1998) argues that IC is composed of three sub-categories of capital: human, structural, and customer/relational (HC, SC and RC). Human capital (human resources plus intellectual assets, according to Edvinsson and Sullivan, 1996) refers to the individual tacit knowledge possessed by the members in an organization, necessary for them to perform their functions, roles and tasks. Individuals' expertise, experience and skills, as well as education, genetic inheritance, and attitudes towards business and life, all contribute to HC. Every node (individual) in a network has a given degree of knowledge. From this, two consequences derive: first, HC is an essential source of strategic renewal (Nahapiet and Ghoshal, 1998); and second, the intelligence of the node is the essence of HC. Structural (or organizational) capital refers to the structural tacit knowledge ingrained in the organization: mechanisms, structures, routines and cultures in an organization, which support individuals

in their quest for superior intellectual performance. SC has a functional role, and facilitates access to information for codification into knowledge. Intellectual assets and know-how exist at the individual level, that are then structured by information systems and other SC into group property (Nicolini, 1993). Customer (or relational) capital relates to the external dimension of organizations and is constituted by knowledge of marketing channels and customers. This form of capital represents the potential that an organization has by virtue of the external intangibles they can mobilise. Examples include relationships with stakeholders, partnerships with the surrounding ecosystem and knowledge transfer initiatives.

This brief review of the literature highlights how central knowledge is to the IC construct. Knowledge builds on a foundation made up of data and information, these three concepts existing in a specific structure. Data constitute raw facts and numbers which, once given meaning, becomes information. This, in turn, becomes knowledge when patterns are recognised within the information (Dretske, 1981). The importance of the relationship between the data-information-knowledge triad and IC has been stressed by Bontis (1998), who has described information as the raw product, knowledge as the finished product and IC as knowledge utilised to produce value. More recently, Tien (2013) maintained the hierarchical nature of the relationship and justified data analysis activities as an attempt to produce information from data; knowledge from information; and wisdom from knowledge.

Other authors conceptualize the data-information-knowledge structure differently. Drawing inspiration from the work of Tuomi (1999), Alavi and Leidner (2001) postulate a bidirectional connection between information and knowledge, whereby the former becomes the latter once processed in an individual's mind and *vice versa*: the latter

becomes the former once articulated and expressed in codified form. The authors contend that knowledge does not exist outside an individual's mind, and can be conceived as a capability. From this, knowledge management is basically intended to create IC. Information systems act in support of knowledge management by developing individual and organizational competencies and reinforcing the fragile knowledge sharing connections naturally existing in organizations (Alavi and Leidner, 2001). At their core, knowledge management systems support the creation, storage and retrieval, transfer and application of knowledge (Schultze and Leidner, 2002).

Knowledge security exists at the intersection between knowledge management and information security and occurs at three levels: products, processes and people (Desouza and Vanapalli, 2005). The sharing economy and its associated digitalisation processes have brought increased opportunities for value-added activities in modern organizations; however, they have also increased widespread concerns around the associated risks, which have been dubbed "knowledge risks" in recent literature (Durst and Zięba, 2017; Zieba and Durst, 2018; Perrott, 2007). In spite of this, research exploring the connections among knowledge, knowledge security, information security and IC is scarce (Desouza, 2006).

Among the first to do so, Bontis (1998) argues that organizations that securely protect their information possess high IC. La Torre, Dumay, and Rea (2018) revisit data, information, and knowledge processes and suggest that protection is needed across all components, for an organization to be able to defend its IC. This is demonstrated by the intrinsic relationship existing, for example, between privacy violations (individual level) and security incidents (organizational level) (La Torre *et al.*, 2018). Extending one of the first attempts to link IC and information security (Renaud et al., 2019), these authors suggest a

framework whereby data breaches impact on IC's traditional components: in particular, loss of confidentiality would affect HC, SC and RC; loss of integrity would affect HC and SC; and so would loss of availability. Despite the originality of their framework, the authors do not empirically test it, and questions around the potential impact that losses of confidentiality, integrity and availability could have on all IC components remain unanswered.

In their literature review, Leal, Meirinhos, Loureiro, and Marques (2017) confirm the scarcity of research on cybersecurity management and IC, a view shared also by Trkman and Desouza (2012). In the latter paper, the researchers raise the trade-off existing between knowledge sharing and knowledge risks and propose their version of the data-information-knowledge tripartite structure: data is the raw input to an interpretive process; information is the aggregation of raw inputs plus application of processing techniques; and knowledge is the collection of experiences, know-how, expertise and gut feelings to help individuals make sense of information.

Knowledge risks are the focus of the study conducted by Zieba and Durst (2018), who, building on a previous paper of theirs (Durst and Zięba, 2017), propose a taxonomy of knowledge risks drawing inspiration from the human-technological-operational perspective. Similar to other researchers, Zięba and Durst (2018) argue that research on knowledge risks is quite limited.

The present study is aimed at filling the literature gaps around the alleged connections among IC, knowledge management and information security. To do so, we explore these topics in the field of higher education, with specific reference to universities.

2.2 Intellectual Capital in Universities

As organizations tasked with producing research and innovation, universities epitomise institutions intensive in intangible assets and IC in general (Paloma Sánchez and Elena, 2006). Moreover, universities are facing three specific challenges, namely an increased demand for transparency on the use of funds, a growing attention to social accountability as a result, among other, of greater autonomy, and expanding competition resulting from lower funding (Secundo *et al.*, 2016). In recent years, universities have seen a growth in their service portfolio beyond traditional teaching and research, and in favour of the "third mission": the need for higher education institutions to open up to the external environment, by transferring knowledge to stakeholders such as private and public organizations, civil society and larger public in general, with the ultimate goal of fostering economic and social growth of their regions and countries (Paoloni *et al.*, 2019; Mariani *et al.*, 2018; Secundo *et al.*, 2018; Etzkowitz *et al.*, 2000). In the light of these trends, activities such as inter-organizational collaboration, open innovation, research commercialisation and public engagement are rapidly diffusing in universities. It is not surprising, therefore, that higher education institutions have attracted a great deal of research on IC and knowledge management practices in general, topics traditionally attached to private organizations (Secundo *et al.*, 2015; Moustaghfir and Schiuma, 2013).

By virtue of these dynamics, a burgeoning stream of literature dedicated to the study of IC components in universities has flourished, leading to the identification of five stages of IC research (Bisogno *et al.*, 2018; Secundo *et al.*, 2018): (1) Identification of IC's interactions with the value creation process in universities; (2) Investigation of evidence to justify the strategic management of IC; (3) Exploration of how universities understand, adapt and apply IC as a management technology; (4) Unpacking of the connection between knowledge

creation inside and outside the organization; and (5) Consideration whether managing IC is even a worthwhile endeavour (Martin-Sardesai and Guthrie, 2018).

For the purposes of this research, an operationalisation of the IC construct is necessary. The canonical, tripartite IC structure proposed by Bontis (1998) is the leading framework, with different nuances based on the individual studies. HC is varyingly defined as explicit and tacit knowledge of personnel (Ramírez *et al.*, 2007) or intangible value in people's competencies (Leitner *et al.*, 2014), and examples include the role of researchers and attracting the best professors and students (Secundo *et al.*, 2015). SC is defined as explicit knowledge associated with internal processes (Ramírez *et al.*, 2007) or intangible resources in the organisation and examples include databases, intellectual property and research projects (Leitner *et al.*, 2014) or publication records of researchers (Secundo *et al.*, 2015). RC is defined as the spectrum of relationships developed by universities (Ramírez *et al.*, 2007) or intangible resources to generate value from internal and external relationships (Leitner *et al.*, 2014) and examples include networks with other universities (Secundo *et al.*, 2015).

A clear-cut taxonomy of the features of IC components in universities is missing in the literature. One of the most compelling challenges for organizations is to translate the knowledge existing at an individual level, to an organizational asset. For this purpose, IC's main function is to organise knowledge resources in a manageable fashion, and this demonstrates the fundamental role of the human dimension of IC (Vagnoni and Oppi, 2015; Secundo *et al.*, 2016). Due to its completeness and granularity, the present research utilises Vagnoni and Oppi's operationalisation of IC as the basis for its conceptual framework. Borrowing from prior work, the two authors combine different nuances to produce the

following tripartite definition of IC, which is complemented by a fourth dimension, connectivity among components (Mariani *et al.*, 2018) (Table I).

Table I here

The next section briefly illustrates some key elements of the dynamics that characterise information security in universities.

2.3 Data, information and knowledge security in universities

Recent events have demonstrated how universities are seen as an increasingly more attractive target for cyber-criminals (Borgman, 2018; Chapman, 2019; Luker and Petersen, 2003). In the United States, in the period January-July 2016, MIT was subject to more than 35 DDoS campaigns (Mejia, 2016). More recently, an investigation conducted by *The Times* in the UK revealed that hundreds of successful cyberattacks have affected top institutions including the Universities of Oxford and Warwick and University College London (Yeung and Bennett, 2017). Besides DDoS attacks or theft of personal identity details (as in the case of social security numbers in the US), there is also growing concern around the potential for sensitive information to be stolen from universities and sold to foreign states, in a cyber-warfare scenario (Yeung and Bennett, 2017).

Universities feature a level of embeddedness for their end-users, which is rarely seen in other organizations. Students are invited to become entrenched (for life, once graduated) as members of the university community. Universities' open-platform architecture makes them particularly vulnerable to external attacks, due to the numerous access points they offer and the extensive amount of data and information they hold at any given time (Liu *et al.*, 2017). With the expansion of activities in which universities are involved ("third

mission"), the types of managed data have been increasing. As data stewards, universities must implement adequate governance mechanisms to achieve the following goals: protecting privacy, guaranteeing academic freedom, defending IP, etc. Such governance mechanisms are, at best, nascent in the university environment (Borgman, 2018). Further, research also shows that diffusion of an adequate information security culture is still incomplete in universities (Hina and Dominic, 2016). Culturally speaking, the higher education environment is characterised by an intrinsic sense of intellectual freedom (Martin-Sardesai and Guthrie, 2018), which stimulates experimentation and open scholarly enquiry and pushes its actors towards information sharing, inter-organizational collaboration, international outreach and individual autonomy (Luker and Petersen, 2003).

A study on information security policies in higher education has highlighted that *personal usage of information* and *Internet access* ranked tenth (second-last) and eleventh (last) in a ranking on the topics mostly covered in information security policies implemented by universities worldwide (Doherty *et al.*, 2009). The same two topics ranked significantly higher (respectively third and second) in a similar ranking in other industries, indicating the different relevance that these topics have.

The costs associated with implementing information security are another issue that IT managers face in modern universities, where pressure on cost containment is often dominant (Lane, 2007). In this environment, information security can easily be perceived as a second priority, when compared to other organizational goals (e.g. work efficiency and effectiveness, Rezgui and Marks, 2008). As a result, universities often embrace the *"least cost and least resistance"* (Lane, 2007) approach to information security, which can negatively impact their security performance.

In summary, arguably, the very nature of the higher education environment presents significant challenges when it comes to ensuring data and information security (Bongiovanni, 2019) and, consequentially, to effectively secure knowledge. Intrinsically, information security and higher education seem prone to have an idiosyncratic relationship, due to their apparently conflicting interests: on the one hand, the need to protect data, information and knowledge; on the other hand, the need seamlessly to share knowledge, to encourage innovation and progress.

3. Research framework

The present research investigates the constituents of IC in universities, with a focus on how higher education institutions can protect HC, SC and RC. We adopt Vagnoni and Oppi's (2015) tripartite structure of IC and posit that HC has a predominant role in universities and a bi-directional relationship with RC (Secundo *et al.*, 2016), and that SC has a support function (Vagnoni and Oppi, 2015; Bontis, 1998). To further operationalise our framework, we utilise Tien's (2013) data-information-knowledge framing (see also Trkman and Desouza, 2012), in its non-hierarchical version (Alavi and Leidner, 2001; Tuomi, 1999). In the present research, data, information and knowledge are considered as *building blocks*, instantiations of HC, SC and RC, whose security is essential to IC protection (Figure 1).

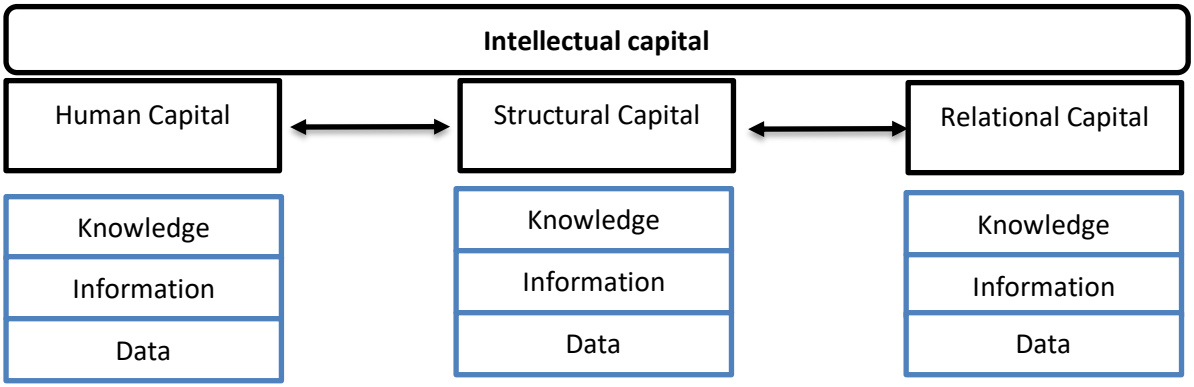

Figure 1: Conceptual framework

Our approach stems from the *interpretive discourse* in studying knowledge management practices (Schultze and Leidner, 2002). Stenmark (2000) argues that in the interpretive discourse, technology can be utilised to formalise tacit knowledge (SC) in organizations where collective action emerge in systems of distributed knowledge (HC). Focus of investigation in interpretive studies is on information systems research. Based on this approach, our study adopted the research methods described in the next section.

4. Research design and methods

This study focused on unpacking issues associated with data, information and knowledge security, as perceived and represented by senior officials in Australian universities. The sample was specifically selected to involve individuals who held both a strategic and an operational role. Being focused on specific senior members with particular organizational responsibilities, the sample selection was partly purposive (Jupp, 2006) and convenience-based (Bryman and Bell, 2015). The final sample of active participants consisted of ten senior officers from research-active, teaching universities across three states in Australia and one individual holding an equivalent position in a public agency undertaking scientific research.

In Australia there are 43 universities (40 Australian universities – 37 public and 3 private - two international campus universities and one Australian university of specialisation). Australian universities are multi-disciplinary, self-governing and, under federal or state and territory legislation, are granted responsibility for their own management, budget, staff, admissions, internal quality assurance and curriculum. In recent years, Australian public universities have been pushed to adopt a corporate managerialism

approach (Christopher, 2014), characterised by efficient use of resources, enhanced institutional management, policy and planning, and increased number of stakeholders to satisfy (Martin-Sardesai and Guthrie, 2018).

Consistent with an interpretive discourse approach (Schultze and Leidner, 2002), our study is qualitative. The format of engagement was therefore designed around a semi-structured interview question set. Prompting questions for the discussions included, among others:

- *What do you think are the critical data and information security risks for your organization?*
- *What factors, in the present, lead you to believe that each of these is critical?;*
- *How do data and information security risks currently inform strategic decision-making in your organization? Why?*

The interviews varied in length from 30 to 75 minutes and were recorded, with permission, and later fully transcribed for content analysis by members of the research team. The research design was subject to institutional ethics approval. Interview analysis was conducted using abductive reasoning (Timmermans and Tavory, 2012), whereby rigorous methodological analysis was used to explore respondents' personal, social and intellectual positions in relation to the subject at hand.

Content analysis of the transcribed interviews was conducted in two stages. The first stage involved *close reading* of the material to identify critical issues identified by individual participants and to group these under common categories. The surfaced categories were then abstracted to relate them to a smaller number of more general, conceptual classes (Miles and Huberman, 1984), using an iterative process of comparison and testing

independently by individual researchers (Spiggle, 1994) before comparison and collation into a single report.

The results of the analysis are outlined and discussed in the following section, in which we link participants' understandings of data and information security risks to extant literature and theory on IC and its components.

5. Findings

The 11 interviewees agreed that data, information and knowledge security represent a superior challenge to universities, as demonstrated by the following excerpt:

> *"You will never going to be on the front foot from a cyber-perspective…the only thing that will give you absolute security and control is disconnecting from the Internet and you put your technology in Fort Knox."* (Resp. 1)

The following sub-section illustrates data, information and knowledge security issues associated with the individual dimension of IC, HC.

5.1 Human Capital

Data revealed that several security threats in universities relate to the experience, perceptions and skills of individuals. Most respondents agreed on the relevance of *spear phishing* (e.g., respondent 10) and, in general, *social engineering* (*"almost on a weekly basis"*, as indicated by respondent 2) as sophisticated ways of exploiting individuals' propensity to fall for luring messages (e.g., emails and messages on social media), for the purpose of extorting personal information (including, for example, credit card details). In universities, spear phishing targets different profiles, including students, academics and professional staff, and its effectiveness is influenced by the ability of such individuals to

recognise it and act accordingly (for example, reporting a suspicious email to the IT department).

In order to gauge the impact that the individual approach to security has on the overall *stock* of IC in the university, one of the interview questions required respondents to elaborate on the nature of data and information security, identifying them as being intrinsically more human or more technical. Interviewees' answers had a two-fold focus: on the one hand, participants elaborated on organizational vulnerability to cyber-threats, an aspect stemming from a SC perspective. However, despite acknowledging the relevance of the technological components (e.g., effectiveness of malwares, structural weaknesses of security architectures), respondents mainly agreed on its predominant human-related nature (e.g., *"…humans are the problem"*, respondent 10). In particular, the topic of end-point vulnerability was extensively discussed:

> *"The consequences of not following good cyber-security practices are probably not well understood."* (Resp. 9)

> *"With the amount of spear-phishing attacks we had in the last six months…we had all the technology sorted, but the way they got in, it's the human clicking…"* (Resp. 5)

The findings presented so far mainly refer to unintentional behaviours by individuals in universities. Several participants also discussed instances in which researchers who operate in research-specific environments that require stability and control, oppose structural security practices, such as *software patching,* which could compromise the integrity of their data. In the case of PhD students, research usually lasts three years and more, and lack of updates for such an extensive timeframe could pose serious security consequences. This tension was represented in the words of one respondent:

"We regularly get pushed back by researchers saying: 'Your controls are too tight, we can't run software or do the experimentation we want to do.'" (Resp. 1)

HC includes consideration of the motivation to act (or not act) in given ways by individuals operating in organizations. Among the most common difficulties that the IT security team encounters, is the complacent attitude of some employees, who do not value data and information security and perceive it as a distraction from their *core business*. In association with instances of SC (e.g., organizational culture), a change in the security attitude of the university was described by most respondents as a slow process. One of the problematic aspects was the disconnect that individuals feel with regards to information security, as represented in the following passage:

"The message should be that cybersecurity is about enabling digital transformation to occur. In this way, cybersecurity would become more meaningful to [people]…but now [cybersecurity] is portrayed as cyber-terrorism…and people disconnect from this." (Resp. 2)

Nonetheless, several respondents acknowledged that their organizations were slowly changing towards a view of cybersecurity, not as a liability but as a source of competitive advantage. This translated into significant differences across universities in terms of staff members dedicated to information security (*"…some universities may have 3-4 people. I've got 15 and a multi-million dollar budget"*; respondent 7), an HC element which contributes to the university's SC.

Specific analysis was needed for *insider threats,* another highly debated topic, reflective of a noteworthy debate happening also in other industries. Respondents highlighted that this threat could possibly take two forms: as the result of malicious

behaviours by individuals; or as unintentional acts committed by employees. Data revealed that the latter form is most common, as demonstrated in the following interviewee's words:

> *"Insiders are not necessarily working for a criminal organization […] it's actually more internal people making poor cybersecurity judgement."* (Resp. 6)

Based on their origin, insider threats can be considered reflective of sub-optimal HC (for example, resulting from poor knowledge of information security) or from adverse effects of RC (for example, when an employee acts upon direction of external, criminal organizations intending to target a specific university). Findings ascribed to the field of HC demonstrate close connections with SC, the main topic of the next sub-section.

5.2 Structural Capital

In general terms, several respondents agreed that the *attack surface* of universities is expanding *("…organizations are increasing their cybersecurity footprint…"*; respondent 2), due to an increasingly multi-modal environment, which significantly spreads data distribution (e.g., BYOD; respondent 9) and raises further challenges in terms of balancing individuals' use of personal devices (HC) with corporate systems (SC). In association with a university's RC, progressively longer supply chains and flexible outsourcing arrangements seem to push the centre of gravity of security controls away from the university premises themselves. In this scenario, it becomes more and more difficult for IT security teams in universities to identify and monitor potential *back-doors* (respondent 1), as these may fall outside the organizational boundaries.

In contrast to this argument, several participants acknowledged the greater flexibility that solutions like cloud computing provide to their customers in universities. A constant quest for flexible solutions, allowing employees to work remotely, in a variety of locations,

together with maintaining the integrity and reliability of their data and information, has facilitated the diffusion of cloud computing. Further, this technological solution was described by respondents as generally efficient, with the potential to alleviate the financial burden on capital expenditure (*CAPEX*) and shift it on operating expenditure (*OPEX*). This last point, in the respondents' words, makes investment in cloud computing (as opposed, for example, to on-premises data centres) also more appealing from a business perspective.

Several respondents acknowledged the diffusion of IoT in universities. While recognising the benefits of real-time data collection deriving from this piece of SC, participants also indicated that its misuse could potentially lead to serious breaches (for example, more effective *Distributed-Denial-of-Service attacks, DDoS*; e.g., respondents 3, 5, and 10), especially considering that universities host an extensive amount of *always connected* devices (e.g., sensors in medical laboratories and robots, but also more traditional devices such as printers, CCTV, etc.). An aspect of IoT was indicated as particularly concerning for universities, namely the increasing exposure deriving from the growing interconnection between the physical and the digital world (*"…the convergence between the information technology and the operating technology"*; respondent 2) that the IoT enables.

> *"IoT is a growing concern: it captures larger amounts of data, imagine for example for research purposes, but there will always be ways to exploit such data."* (Resp. 3)

Concerns around IoT epitomised an underlying issue mentioned by numerous respondents in the interviews, the juxtaposition of present-day IT capabilities with legacy-systems that are still largely present in modern universities. One participant illustrated the *contagion effect* intrinsic to having a previously physical-only, standalone device, for which

data and information security was not built-in, transformed into a gateway for a larger digital network (respondent 5). On the same topic, respondent 3 witnessed that architectures with in-built security can be more easily developed utilising *"green-field"* components, as opposed to legacy ones. In the respondent's words, the latter can only have *"tagged-on"* (and not built-in) security.

Besides the role of technology in protecting (or jeopardizing) the security of data, information and knowledge in universities, participants elaborated on another component of SC, namely organizational practices and structures aimed at preserving the confidentiality, integrity, and availability of information. These arguments often revolved around the consideration whether information security could be considered an operational or a strategic activity performed in universities. Consistently with current debates in other industries, interviewees agreed that a "strategic turn" is indeed necessary for information security to receive the necessary consideration in universities. In the interviewees' words, one of the most powerful leverages to ease this transition is raising awareness around the destructive impact that security breaches can have on organizations.

In close connection with RC, reputational risks are generally perceived as particularly significant for universities, especially with the current, expanding student bases. Respondents explained that the reputational aspect of data and information security is particularly debated in the board of directors' meetings (SC). However, most participants believed that data and information security are still seen as an operational issue, rather than a strategic one, in the sense of conducive of shifts in the competitive balance. Because of this, interviewees concluded that information security is perceived as a risk management issue, for which mitigation attracts the most effort in terms of SC.

"I think for an organization such as ours, [information security] is still a risk management issue, I think it will drive eventually towards strategic, but it's something that is a cultural change and I think it takes time." (Resp. 5)

This scenario could mutate if a major security incident happened, which would likely push towards a change in mindset, as witnessed by respondent 3. However, with lack of practical examples on the implications that a security breach could have, respondents explained that justifying information security expenditure is a challenging task, especially when the board of directors and the IT security team speak different languages, with the former more business-minded and the latter more technically-oriented.

"As an IT manager, how do you communicate with company directors in non-technical ways, as they usually do not come from an IT background?" (Resp. 3)

Generally, interviewees agreed that return on investment on information security is difficult to demonstrate and several of them argued that their board of directors could prefer taking some limited risks, rather than over-investing in information security. One of the arguments to justify this stance, the respondents illustrated, was that growth is enabled by taking acceptable levels of risk, especially in the university sector, naturally prone to innovation. In the same direction, data and information security, as with any other risk management investment, may require significant money and not deliver tangible results other than avoiding major losses.

"The boards of directors are looking at growth, and there is no growth without risk…and sometimes they might go: 'Is IT crying wolf yet again?'… It's a very fine line." (Resp. 1)

Concerns were also raised about the potentially cyclical pattern of information security investments, whereby the current hype around cybersecurity could wane when other priorities emerge:

> *"Maybe in two years' time someone may be: 'Well, security had enough money in the last years, now it's time to invest in something else.'"* (Resp. 11)

5.3 Relational Capital

The complex nature of relationships that universities have with service providers emerged, especially in the field of data and information security. Service level agreements allow IT departments to ensure some control over vendors' activities, at least in terms of business continuity management in case of a breach of contractual terms. Contract management was therefore considered a crucial component of data and information security, to the point that one participant argued that one of the main duties of the IT department is managing vendors, and not IT itself (respondent 5).

Respondents also indicated that one way to ensure enhanced control is to only engage with vendors based in Australia, in order to keep data onshore and ensure compliance with Australian legislation. The interviews, however, showed that effective contract management is a challenging objective, mainly due to the difficulty in assessing vendors' security performance. One respondent argued that they would love to completely outsource the information security function, should they identify a vendor capable of ensuring outstanding security at a reasonable price (respondent 3). Finally, on a higher level of abstraction, when discussing contract management, several respondents elaborated on an essential component of RC, trust, and the role it has in managing contracts with third-parties:

"In cloud services, trust is earned." (Resp. 5)

"[Third-party] contracts are a proxy for trust, but they're not a perfect one." (Resp. 3)

Regardless of the level of trust embedded in the delivery of security services, respondents expressed concerns around the erosion of control (and security) that apparently comes with technological solutions such as cloud applications, as witnessed in the following excerpt:

"Cloud computing is a reality of life, and it's a two-edged sword as it offers benefits…But you also lose some controls…when the updates are being done? How do you manage your data…how do you know how secure [the vendor] is?" (Resp. 3)

To conclude on the impact on RC that data and information security has in universities, respondents also discussed the implications of the current push for internationalisation. The increase in international travel by individuals in universities requires consideration of the security repercussions of carrying and utilising university-owned devices abroad. One mentioned instance was the case of researchers accessing public Wi-Fi networks in foreign countries where, for example, regulations on cybersecurity are less stringent (respondent 4).

5.4 Other data, information and knowledge security issues

The interconnected nature of IC's components was confirmed, in the form of topics whose nature cuts across HC, SC and RC. Several respondents discussed the importance of data and information security awareness in universities and described it as an organizational reaction (SC) to phenomena that are eminently individual (HC). Interviewees illustrated that, at the end-point level, the university environment shows all its diversity, with several categories of users coming from different cultural backgrounds and having different views on data and

information security (e.g., *"…we manage over 100,000 identities"*; respondent 7). From the interviews, it emerged how this complexity of profiles renders a standardised, one-size-fits-all approach to end-point security only partially effective. Consequently, interviewees stressed the importance of working on the individual information security awareness (HC) to lift the security culture of all users (SC). Respondents mentioned different practices used in their universities to raise information security awareness. All of them, however, agreed that such practices need to be complementary, and the best way to increase awareness is by providing a mix of methods, as represented in the following excerpt.

> *"We try to keep [information security] front of mind, it's a deliberate campaign, but it's not just posters splashed around the walls, it's more a mindset of a culture about whatever we do, it needs to be safe."* (Resp. 4)

Respondent 9 explained that in their organization, a first approach to information security awareness is by launching internal campaigns, organising events, and conducting information security training in general. A second phase requires one-on-one contact with the university players, for the IT security managers to account for the diversity of their *customers* (e.g., academics and students) and customise information security awareness to their needs and capabilities. However, the generally scarce resources dedicated to information security render this exercise hardly sustainable, considering the high number of individuals to approach. As a result, as mentioned by one interviewee, often external media reports on eminent cyber-breaches (potentially impacted by the stock of RC a university holds) have a higher impact on employees than internal training practices.

Considerations were made by respondents on the different availability of knowledge held by internal and external actors to universities, with current trends potentially posing

relevant challenges for the "defenders". In general, participants noted that malicious tools on the *dark web* (in particular, re-purposed government surveillance tools) are relatively easy to access and use, which increases the number of potential attackers and gives them a competitive edge over IT security managers (Respondent 3).

> *"Anyone can be a hacker. Kids coming out of school have much more IT knowledge than people that just graduated a couple of years ago."* (Resp. 4)

External factors did not only refer to the malicious intent of attackers, but also to the surrounding social, economic and legal environment and how this had the potential to affect IC held by universities. One of the interview questions asked respondents to elaborate on the impact that legislation[1] would have on data and information security in Australia. Opinions on this matter were generally aligned around the positive impact that such legislation would have on raising awareness on security. This question also yielded some broader considerations on the Australian culture which, in one respondent's words, is *"woeful"* when it comes to discussing risks and, in general, is not naturally prone to disclosure (respondent 2).

6. Discussion

Our findings confirm that securing data, information and knowledge in universities is challenging. From an IC perspective, universities are characterised by a prominent role of HC, whereby knowledge residing with individuals is influenced by their role within the organization and by their background (e.g., prior experience and culture). Given the variety of profiles existing in universities, ranging from specific roles (e.g., academics, professional staff, students, other stakeholders) to cultural differences (e.g., the push to

[1] Such as the *Notifiable Data Breaches scheme,* which obliges organizations affected by data and information security breaches to disclose such breaches.

internationalisation, which has broadened the spectrum of cultures operating in higher education), HC takes numerous forms, and its assessment has to account for such variety.

An interesting finding of the present research relates to the impact that sub-optimal knowledge at the individual level has on the security of data and information in universities. Participants in our interviews emphasised that end-users in universities have very different understanding of information security practices: behaviours that for some may be legitimate (e.g., sharing data on non-accredited cloud platforms), for others are a clear violation of corporate security policies. As a result, individual knowledge *qualitatively* impacts the overall amount of HC (and IC) in a university, which suggests that assessing HC requires reflecting on the adequacy/non-adequacy of individual tacit knowledge in an organization, not just its presence/absence. This finding is consistent with literature stressing the importance of calculating HC loss (besides acquisition) in higher education institutions (Martin-Sardesai and Guthrie, 2018).

On this note, a first conceptual bridge between HC and SC is built by our research. The senior IT managers highlighted the importance of information security training in establishing (and then elevating) shared security awareness, a *level playing field* among end-users in universities: such training, as codified knowledge existing in an organization (SC) is used to influence and improve tacit knowledge held at the individual level (HC). *Vice versa*, the quality of individual knowledge serves as a *scale* to weight and customise security training programs and courses. This suggests that HC and SC have a symbiotic relationship in universities.

The present research postulated that data and information, together with knowledge, constitute instantiations of HC. The results of our analysis demonstrate that, by

virtue of a diffused *ethos* of academic freedom and the multi-modal nature of universities (Martin-Sardesai and Guthrie, 2018; Borgman, 2018), individuals enjoy a significant degree of control over the data and information they collect, store and produce in higher education institutions. Compared to other public and private organizations, the boundaries between individual and organizational IP are fuzzier in universities, to the point at which HC created in one institution in the form of data or information (e.g., a research project), could be translated into knowledge in another institution (e.g., when the investigator moves to another university). Similarly, the resulting knowledge could be formalised as SC in a third university (e.g., when the investigator moves to another university and publishes a paper based on research conducted previously). These dynamics highlight, once again, the challenges existing with regards to HC and SC protection in higher education.

Defined as *"knowledge that stays within the firm at the end of the working day"* (Meritum, 2002, p. 11), SC represents the purest organizational form of knowledge present in a university. Due to their role as senior IT managers, our interviewees mainly elaborated on two elements of SC: technology and organizational practices to secure data, information and knowledge. Our findings highlight that a combination of the two is necessary to ensure security in universities. In particular, the need to complement traditional, technical defences (e.g., IT security architecture) with organizational, human-focused interventions (e.g., awareness campaigns) is widely recognised in universities, and so is scepticism for centralised, *one-size-fits-all* solutions. This is consistent with recommendations in the literature that higher education institutions should avoid centralised information security models typical of corporate IT departments in favour of *"embraced autonomy"* (Adler, 2006, p. 58), a model that aligns universities' asymmetric structure with active participation and engagement in the information security efforts by their constituents (e.g., campuses,

branches, colleges, departments, etc.). Conceptually, investing in technology and virtuous security practices translates into investments in SC. Our research suggests senior IT managers to utilise this framing as a promising perspective for conversations around information security budgeting with university management, perhaps more receptive to a business-based (and not a technical) approach to security.

Existing literature argues for a support role of SC, which facilitates the development of HC and RC (Vagnoni and Oppi, 2015; Bontis, 1998). Data collected in this research seem to align with this: respondents extensively discussed the functional role of technology and organizational practices in promoting organizational activities and in building a solid network of external stakeholders. Similar to HC, SC is instantiated through data, information and knowledge at the organizational level: a research dataset owned by a university department; a scientific report elaborated from such dataset; and the associated expertise residing with a research team. Again, assessing SC entails evaluating the quality (and not just the quantity or the size) of the data, information and knowledge produced at the SC. Interestingly, however, negative events affecting SC and its instantiations seem to have the potential for superior adverse effects than similar events affecting HC: an example is the case in which an ill-designed information security policy is diffused through training throughout the university, or a malicious external agent (e.g., a hacker) has access to a database of login credentials. This further corroborates the support function of SC.

Universities' roles as innovation hubs within an ecosystem of public and private organizations, civil society and other constituencies pertains to their RC, a topic only recently discussed in the field of higher education (Paoloni *et al.*, 2019). The emergence of universities' third mission (Etzkowitz *et al.*, 2000) has brought increased focus on how to

secure the portion of IC capital deriving from connections with the outside world. Several respondents in our research demonstrated solid awareness of issues associated with the protection of IP from malicious external actors, often sponsored by state government or private companies. Just like for HC and SC before, this element entails the need to consider the adequacy of RC in universities, and not just its presence/absence. The acknowledgement of an increased role for universities in national and international ecosystems comes with the growing importance that reputation, as one of the foundations of trust, has for such institutions. In this sense, a breach in the data, information and knowledge security systems of universities can yield significant consequences in terms of lost trust, reputation and relational capital. Unlike La Torre, Dumay and Rea (2018), we argue that regardless of data breaches' nature (as loss of confidentiality, integrity or availability of information), impacts on RC through reputational damage are always possible.

The very organizational boundaries of universities appear vaguer, when compared to other public and private organizations. Based on our data, we have identified two types of "embeddedness" that characterise the organizational fabric of universities. *Vertical embeddedness* refers to the integration that different categories of end-users (mainly students, academics, professional staff and stakeholders "sitting on the fence") have within a university. Vertical embeddedness manifests at both the HC and SC levels. In terms of HC, universities have different categories of end-users; traditional provider-costumer roles are ill-defined and students are arguably at the same time *clients* (they pay fees to obtain a degree) and *providers* (they produce knowledge in the form of, for instance, assignments, which are forms of HC).

In addition to this, individuals have different degrees of understanding and perceptions of data and information security. In terms of SC, they all have access to basic shared facilities and technologies and all act upon established security policies and practices. The dynamics associated with vertical embeddedness originate therefore at the HC level but, given the configuration of universities, have the potential for adverse events such as data and information security breaches at the SC. To tackle this, the different degrees of understanding of information security (HC) would require a customised approach to information security management (e.g., training, SC). Yet, this usually does not happen in universities; training is administered with a *blanket* approach that does not feasibly account for end-users' nuances.

Horizontal embeddedness refers to the inter-organizational integration that exists across higher education institutions and other public and private organizations, in the light of increasing international collaboration and third mission activities. Horizontal embeddedness manifests at both the RC and SC levels. In terms of RC, universities promote practices such as students being involved in international exchange programs; academics sharing datasets and co-producing research across countries, or being invited as *visiting academics* in different institutions; and non-academic staff members working on strategic partnerships around topics such as accreditation or education delivery (e.g., *Massive Open Online Courses, MOOCs*). In terms of SC, these practices are accompanied by supportive efforts, and investments, such as the award of joint degrees, the creation of shared IT networks (for example, *Eduroam*), the constitution of grants aimed at promoting international collaboration, the promotion of knowledge exchange with public and private companies, etc. The dynamics of horizontal embeddedness originate at the RC level, but have the potential for data and information security breaches to manifest at the SC. Figure 2

represents the relationships among vertical and horizontal embeddedness and the components of IC.

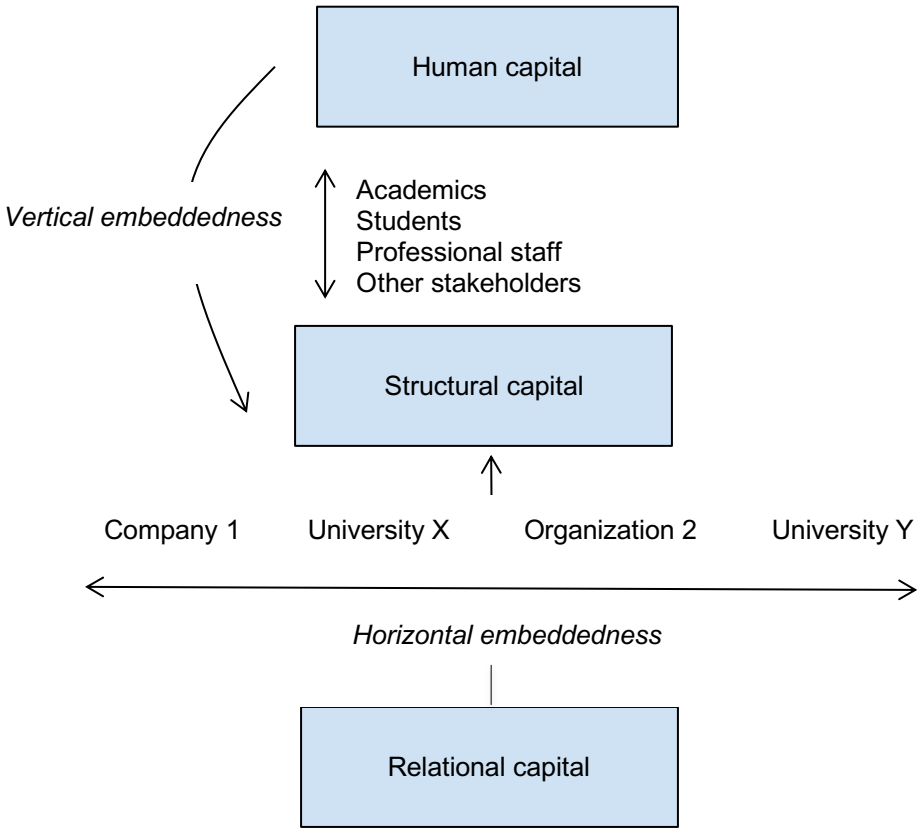

Figure 2: IC components and vertical/horizontal embeddedness in universities

6.1 Research implications

The implications of our findings are*, first*, that the roles played by the actors in universities have the potential to impact the quality of HC held by the university at any given moment. We therefore recommend that future studies on HC in higher education account for the typical university profiles (students, academics, professional staff and other stakeholders) and their specificity *vis-a-vis* the contribution to, or erosion of, HC (vertical embeddedness). *Second*, the specific characteristics of organizations and other constituencies interacting with universities have the potential to influence the quality of RC. Profiling such

characteristics in a discrete taxonomy (horizontal embeddedness) is a much more complex task than for HC, and we recommend that, at least, future studies assessing RC in higher education consider the relationships between a university and its external partners based on the nature of the involved activities: teaching, research, service, and third mission. *Third*, we suggest that future studies aimed at assessing SC in universities account for the role and influence of HC and RC.

From a practical perspective, this research provides senior IT security managers with an original framework to illustrate the potential adverse effects that poor data, information and knowledge security may have on universities' IC, as declined in its three components. Such framework can be fruitfully utilised to substantiate these concepts before executive members in universities, who do not necessarily have solid knowledge in information security management.

6.1 Limitations and future research

Like any other, the present research has limitations. First, the adopted key informant methodology has the potential to suffer from potential biases (Kumar *et al.*, 1993). In our study, we interviewed senior IT managers, who have mainly contributed in the field of SC. However, this individuals' function is embedded in the component of IC around which HC and RC pivot. Their selection seemed therefore an efficient way to gather meaningful information, conducive of a holistic view on IC. Second, our sample represents around 25% of the population of Australian universities from three (out of 7) States and Territories in the country. Future research is recommended to expand the sample, to control for possible factors associated with state legislation. Third, our findings should be tested by means of a quantitative investigation. A large-scale survey designed around the results of the present

paper is a possible avenue. Fourth, our results represent the Australian case. Given the impact that country-specific factors (e.g., legislation, governance in higher education, funding models, etc.) could have on the findings, we recommend similar studies in other countries. To this end, we have plans to conduct a similar study in universities and research centres in the United Kingdom and in South Africa.

7. Conclusions

This research has contributed to the third and fourth stages of research on IC (Secundo *et al.*, 2018), by demonstrating that the complexity of IC in higher education institutions goes beyond the tripartite structure of IC. It has done so by unpacking the elements of HC, SC and RC, confirming, as argued in the literature (Vagnoni and Oppi, 2015), the importance of the relationship among such components (connectivity) as a fourth element. Our research has explored the connection existing between IC and its various instantiations in universities' data, information and knowledge, highlighting the crucial nature of information security structures and measures in protecting the organization's IC and ensuring that they can benefit from this crucial asset.

Acknowledgements

Data collection for this research was carried out during the first author's appointment at the QUT Business School (Brisbane, QLD, Australia). The authors would like to acknowledge and thank George Cairns, retired academic and formerly Adjunct Professor at QUT Business School, who significantly contributed to a previous version of this paper.

Funding

This research did not receive any specific grants from funding agencies in the public, commercial, or not-for-profit sectors.

References

Adler, M. P. (2006) "A Unified Approach to Information Security Compliance", *Educause Review,* 41(5), 46.

Alavi, M. and Leidner, D. E. (2001) "Knowledge management and knowledge management systems: Conceptual foundations and research issues", *MIS Quarterly*, 107-136.

Asiaei, K. and Jusoh, R. (2015) "A multidimensional view of intellectual capital: the impact on organizational performance", *Management decision,* 53(3), 668-697.

Bisogno, M., Dumay, J., Manes Rossi, F. and Tartaglia Polcini, P. (2018) "Identifying future directions for IC research in education: a literature review", *Journal of intellectual capital,* 19(1), 10-33.

Bongiovanni, I. (2019) "The least secure places in the universe? A systematic literature review on information security management in higher education", *Computers & Security,* 86, 350-357.

Bontis, N. (1998) "Intellectual capital: an exploratory study that develops measures and models", *Management decision,* 36(2), 63-76.

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

Bryman, A. and Bell, E. (2015) *Business research methods,* Fourth ed*.,* Oxford: Oxford University Press.

Chapman, J. (2019) *How safe is your data? Cyber-security in higher education*, 12, Oxford, UK: Higher Education Policy Institute,.

Christopher, J. (2014) "Australian public universities: are they practising a corporate approach to governance?", *STUDIES IN HIGHER EDUCATION,* 39(4), 560-573.

Desouza, K. C. (2006) "Knowledge Security: An Interesting Research Space", 25.

Desouza, K. C. and Vanapalli, G. K. (2005) "Securing knowledge in organizations: lessons from the defense and intelligence sectors", *INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT,* 25(1), 85-98.

Di Berardino, D. and Corsi, C. (2018) "A quality evaluation approach to disclosing third mission activities and intellectual capital in Italian universities", *Journal of intellectual capital,* 19(1), 178-201.

Dierickx, I. and Cool, K. (1989) "Asset stock accumulation and sustainability of competitive advantage", *Management science,* 35(12), 1504-1511.

Doherty, N. F., Anastasakis, L. and 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.

Dretske, F. (1981) "Knowledge and the Flow of Information".

Durst, S. and Zięba, M. (2017) "Knowledge risks-towards a taxonomy", *International Journal of Business Environment,* 9(1), 51-63.

Edvinsson, L. and Sullivan, P. (1996) "Developing a model for managing intellectual capital", *European management journal,* 14(4), 356-364.

Etzkowitz, H., Webster, A., Gebhardt, C. and Terra, B. R. C. (2000) "The future of the university and the university of the future: evolution of ivory tower to entrepreneurial paradigm", *Research policy,* 29(2), 313-330.

Hina, S. and Dominic, D. D. (2016) *Information security policies: Investigation of compliance in universities,* translated by Kuala Lumpur: IEEE, 564-569.

Jupp, V. (2006) *The SAGE dictionary of social research methods,* Thousand Oaks, CA: SAGE Publications.

Kumar, N., Stern, L. W. and Anderson, J. C. (1993) "Conducting Interorganizational Research Using Key Informants", *The Academy of Management Journal,* 36(6), 1633-1651.

La Torre, M., Dumay, J. and Rea, M. A. (2018) "Breaching intellectual capital: critical reflections on Big Data security", *Meditari Accountancy Research,* 26(3), 463-482.

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

Leal, C., Meirinhos, G., Loureiro, M. and Marques, C. (2017) *Cybersecurity Management, Intellectual Capital and Trust: A New Management Dilemma,* translated by 171-181.

Leitner, K.-H., Elena-Pérez, S., Fazlagić, J., Kalemis, K., Martinaitis, Ž., Secundo, G., Sicilia, M.-A. and Zaksa, K. (2014) *A Strategic Approach for Intellectual Capital Management in European Universities. Guidelines for Implementation*.

Liu, C.-W., Huang, P. and Lucas, H. (2017) *IT Centralization, Security Outsourcing, and Cybersecurity Breaches: Evidence from the US Higher Education,* translated by Library, A. I. S. E., Seoul, South Korea: AIS Electronic Library.

Luker, M. A. and Petersen, R. J. (2003) *Computer and network security in higher education,* San Francisco, CA: Jossey-Bass.

Mariani, G., Carlesi, A. and Scarfò, A. A. (2018) "Academic spinoffs as a value driver for intellectual capital: the case of the University of Pisa", *Journal of intellectual capital,* 19(1), 202-226.

Martin-Sardesai, A. and Guthrie, J. (2018) "Human capital loss in an academic performance measurement system", *Journal of intellectual capital,* 19(1), 53-70.

Mejia, W. (2016) *Case Study: Time Line of DDoS campaigns against MIT*, Akamai.

Meritum (2002) "Guidelines for managing and reporting on intangibles", *Fundación Airtel-Vodafone*.

Miles, M. B. and Huberman, A. M. (1984) "Drawing Valid Meaning from Qualitative Data: Toward a Shared Craft", *Educational Researcher,* 13(5), 20-30.

Moustaghfir, K. and Schiuma, G. (2013) "Knowledge, learning, and innovation: research and perspectives", *Journal of knowledge management,* 17(4), 495-510.

Nahapiet, J. and Ghoshal, S. (1998) "Social capital, intellectual capital, and the organizational advantage", *Academy of Management Review,* 23(2), 242-266.

Nicolini, D. (1993) "Apprendimento organizzativo e pubblica amministrazione locale", *Autonomie Locali e Servizi Sociali,* 16(2), 277-287.

Paloma Sánchez, M. and Elena, S. (2006) "Intellectual capital in universities: Improving transparency and internal management", *Journal of intellectual capital,* 7(4), 529-548.

Paloma Sánchez, M., Elena, S. and Castrillo, R. (2009) "Intellectual capital dynamics in universities: a reporting model", *Journal of intellectual capital,* 10(2), 307-324.

Paoloni, P., Cesaroni, F. M. and Demartini, P. (2019) "Relational capital and knowledge transfer in universities", *Business Process Management Journal,* 25(1), 185-201.

Perrott, B. E. (2007) "A strategic risk approach to knowledge management", *Business Horizons,* 50(6), 523-533.

Quinn, J. B. (1992) *Intelligent Enterprise: A Knowledge and Service Based Paradigm for Industr,* Simon and Schuster.

Ramírez, Y., Lorduy, C. and Rojas, J. A. (2007) "Intellectual capital management in Spanish universities", *Journal of intellectual capital,* 8(4), 732-748.

Renaud, K., Von Solms, S. and Von Solms, R. (2019) “How does Intellectual Capital Align with Cyber Security?” Journal of Intellectual Capital, 20(5), 621-641. https://doi.org/10.1108/JIC-04-2019-0079

Rezgui, Y. and Marks, A. (2008) "Information security awareness in higher education: An exploratory study", *Computers & Security,* 27(7), 241-253.

Schultze, U. and Leidner, D. E. (2002) "Studying knowledge management in information systems research: discourses and theoretical assumptions", *MIS Quarterly*, 213-242.

Secundo, G., Dumay, J., Schiuma, G. and Passiante, G. (2016) "Managing intellectual capital through a collective intelligence approach: an integrated framework for universities", *Journal of intellectual capital,* 17(2), 298-319.

Secundo, G., Elena-Perez, S., Martinaitis, Ž. and Leitner, K.-H. (2015) "An intellectual capital maturity model (ICMM) to improve strategic management in European universities: A dynamic approach", *Journal of intellectual capital,* 16(2), 419-442.

Secundo, G., Massaro, M., Dumay, J. and Bagnoli, C. (2018) "Intellectual capital management in the fourth stage of IC research: A critical case study in university settings", *Journal of intellectual capital,* 19(1), 157-177.

Spiggle, S. (1994) "Analysis and Interpretation of Qualitative Data in Consumer Research", *Journal of Consumer Research,* 21(3), 491-503.

Stenmark, D. (2000) "Leveraging Tacit Organizational Knowledge", *Journal of Management Information Systems,* 17(3), 9-24.

Stewart, T. A. (1998) *Intellectual Capital: The New Wealth of Organizations,* Nicholas Brealey.

Tien, J. M. (2013) "Big data: Unleashing information", *Journal of Systems Science and Systems Engineering,* 22(2), 127-151.

Timmermans, S. and Tavory, I. (2012) "Theory Construction in Qualitative Research: From Grounded Theory to Abductive Analysis", *Sociological Theory,* 30(3), 167-186.

Trkman, P. and Desouza, K. C. (2012) "Knowledge risks in organizational networks: An exploratory framework", *The Journal of Strategic Information Systems,* 21(1), 1-17.

Tuomi, I. (1999) *Data is more than knowledge: Implications of the reversed knowledge hierarchy for knowledge management and organizational memory,* translated by IEEE, 12 pp.

Vagnoni, E. and Oppi, C. (2015) "Investigating factors of intellectual capital to enhance achievement of strategic goals in a university hospital setting", *Journal of intellectual capital,* 16(2), 331-363.

Yeung, P. and Bennett, R. (2017) "University secrets are stolen by cybergangs", *The Times* [online], available: https://www.thetimes.co.uk/article/university-secrets-are-stolen-by-cybergangs-oxford-warwick-and-university-college-london-r0zsmf56z [accessed 1 March 2018].

Zieba, M. and Durst, S. (2018) "Knowledge risks in the sharing economy" in *Knowledge management in the sharing economy*, Springer, 253-270.