View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Abertay Research Portal

How does intellectual capital align with cbyer security?

Karen Renaud
Basie von Solms
Rossouw von Solms

This is the Author Accepted Manuscript. The final published version is available at Emerald via doi: https://doi.org/10.1108/JIC-04-2019-0079

How does Intellectual Capital Align with Cyber Security?

Karen Renaud
Abertay University, Dundee, U.K.
University of South Africa,
South Africa
k.renaud@abertay.ac.uk

Basie von Solms
University of Johannesburg,
Johannesburg, South Africa
basievs@uj.ac.za

Rossouw von Solms
Nelson Mandela University,
Port Elizabeth, South Africa
rossouw@mandela.ac.za

Structured Abstract:

Purpose – To position the preservation and protection of intellectual capital as a cyber security concern. We outline the security requirements of intellectual capital to help Boards of Directors and executive management teams to understand their responsibilities and accountabilities in this respect.

Design/Methodology/Approach – The research methodology is desk research. In other words, we gathered facts and existing research publications that helped us to define key terms, to formulate arguments to convince BoDs of the need to secure their intellectual capital, and to outline actions to be taken by BoDs to do so.

Findings – Intellectual capital, as a valuable business resource, is related to information, knowledge and cyber security. Hence, preservation thereof is also related to cyber security governance, and merits attention from boards of directors.

Implications – This paper clarifies boards of directors' intellectual capital governance responsibilities, which encompass information, knowledge and cyber security governance.

Social Implications – If boards of directors know how to embrace their intellectual capital governance responsibilities, this will help to ensure that such intellectual capital is preserved and secured.

Practical Implications – We hope that boards of directors will benefit from our clarifications, and especially from the positioning of intellectual capital in cyber space.

Originality/Value – This paper extends a previous paper published by Von Solms and Von Solms (2018), which clarified the key terms of information and cyber security, and the governance thereof. The originality and value is the focus on the securing of intellectual capital, a topic that has not yet received a great deal of attention from cyber security researchers.

Keywords – Intellectual Capital, Intellectual Capital Security Governance, Boards of Directors, Executive Management Teams.

Paper type – Viewpoint.

1. Introduction

Rastogi (2002) claims that an organization's *Intellectual Capital* (IC) is extremely valuable, as valuable as any of its other assets. Dierickx and Cool (1989) argue that IC is actually the *most* valuable organizational resource, giving an organization its competitive advantage. There is evidence that IC makes up a large percentage of a company's market value (Blair and Wallman, 2000). Organizations routinely act to protect and secure their tangible information assets (Elson and LeClerc, 2006), so it makes sense that they should also act to protect and secure their IC assets.

It is important for Boards of Directors (BoDs) and executive management teams to understand the extent of their cyber-related responsibilities (Von Solms and Von Solms, 2018). Here, we argue that these cyber responsibilities also include the protection and securing of IC, as a valuable, yet often intangible, asset. Consider that most organizations of the 21st century utilize cyber space for critical business processes and relationship management, and have become increasingly reliant on these new technologies (Goel and Sunena,

2018). The underlying infrastructure, the Internet, has very rapidly become an integral link in modern information systems and a ubiquitous business enabler (Sukhodolov *et al.*, 2018).

As a consequence, BoDs' roles and responsibilities have changed significantly over the last few decades (Flyverbom *et al.*, 2019): they now have a mandate also to take responsibility for cyber security governance. Yet they do not necessarily appreciate the extent of their cyber responsibilities (Trautman, 2016). This relatively new responsibility makes BoDs and executive management teams nervous (Sims, 2019; Abraham *et al.*, 2019). Only a third of IT professionals believe that board members really understand the cyber field (Bay Dynamics, 2015), probably because, despite cyber's ubiquity in modern organizational usage, the core concepts are poorly defined and understood (Ramirez and Choucri, 2016). This lack of clarity gets in the way of organizations achieving their objectives (Althonayan and Andronache, 2018). In a world where data breaches occur far too often, it is important for BoDs to appreciate the full extent of their cyber-related governance responsibilities.

IC is clearly a valuable organizational asset (Bontis, 2000). Yet IC is also a far more complicated and intangible concept than information (Turner *et al.*, 2015). De Santis and Presti (2018) [p. 361] call IC a "*multifaceted and heterogeneous concept*". We shall demonstrate that it has both informational and knowledge aspects, thus making the preservation and securing thereof challenging. We will also argue that IC can be leaked via the Internet, meaning that it is necessary to explore the role of BoDs when it comes to the intersection of IC and cyber security governance.

Von Solms and Von Solms (2018) have already written a similar treatise highlighting the core concepts of cyber space and delineating the cyber-related remit of BoDs. Why do we need to extend their discussion? We believe it is both helpful and valuable to consider how IC fits in, because, in a modern knowledge-based economy (Powell and Snellman, 2004) with hyper-connectivity via the Internet, BoDs need to govern the security of *all* their valuable assets, including IC.

To maximize the clarity of our discussion, we take the same approach as that taken by Von Solms and Von Solms (2018), who argue that simple and understandable definitions of the key terms in the cyber security space be provided, and that a clear delineation of BoD responsibilities be outlined. Here we extend their discussion to include IC security too.

We first present the underlying concepts from Von Solms and Von Solms' (2018) paper in Section 2 to ground our discussion in the foundational terms. We then turn our attention to the concept of "intellectual capital", providing a definition and positioning it within cyber space in Sections 3 and 4. Section 5 consolidates the previous sections into a clear and concise message for BoDs and executive management teams. We also provide a list of cyber-related actions to be taken by boards in this respect. Section 6 concludes.

2. Information Security & Cyber Security, what goes where? (Von Solms and Von Solms, 2018)

Cyber security, as a topic, attracts considerable interest and attention from a wide spectrum of stakeholders (Martin and Rice, 2011). It is growing in importance and significance, with ever-expanding, long-term consequences and impacts (McMillan, 2019; Bianchi and Tosun, 2019). Stakeholders span the full spectrum – from the ordinary citizen using online banking, to companies' BoDs to nation states. BoDs are coming to the realization that protecting their respective companies' presence in cyber space is a corporate governance responsibility that cannot be delegated or neglected (Wootliff, 2019). BoDs are held accountable for the related cyber risks in their companies, together with the associated subsequent legal implications for possible negligence and/or ignorance (Zukis, 2019). The recent enactment of the European GDPR regulation (EU Parliament, 2018), with the punitive financial fines that can be imposed in the aftermath of data breaches, make the topic even more relevant in Europe. Other countries have similar legislation (e.g. Californians for Consumer Privacy, 2018; Michaelsons, 2018), reflecting the global importance of this topic.

Von Solms and Von Solms (2018) define *information security* and outline its relationship with the newer *cyber security*. Having delineated these topics, they also consider the differences between *information* security and

cyber security governance. We include definitions for these concepts here, because they help to contextualize the subsequent IC security discussion. To ensure clarity of communication of the core concepts at this moment in time, we have retained the original definition used by Von Solms and Von Solms.

> **Information security** can be defined as "*the preservation of the confidentiality, integrity and availability of information.*" (derived from the ISO/IEC 27000 standard and included in Von Solms and Von Solms (2018) [p. 4]).

The *confidentiality*, *integrity* and *availability* properties are referred to as the "CIA properties" of information. We can now define the governance concept:

> **Information security governance** is defined by Von Solms and Von Solms (2018) [p.4] as "*the governance of information security, regardless of its format*."

We now provide definitions of the *cyber* terms.

> Schatz *et al.* (2017) [p.66] define **cyber security** as "*the approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space.*"

Note the mention of the same CIA properties in the cyber security definition as we see in the information security definition. Having positioned cyber security within the information security domain (but not encompassing it), Von Solms and Von Solms conclude that ***cyber security governance*** is also a subset of information security governance (Von Solms and Von Solms, 2008) [p.6], defining it as:

> *"the process of directing and controlling the protection of a company's digital information assets from the risks that are related to using the Internet."*

The key insights to be drawn out of these definitions are that information security is related to preserving the CIA properties of information (regardless of format), while cyber security covers these activities within cyber space (where the format is digital), thereby resisting *Internet-enabled* threats and attacks. Concept-specific governance definitions also reflect this difference.

Some examples serve to clarify the impact of the definitions.

- A company pays a contractor to destroy the hard drives of computers they want to dispose of. The contractor chooses, instead, to sell the hard drives on an online auction store (BBC, 2013). This is a breach of digital *information security*, but not of *cyber security*; as the Internet is not involved in the breach.
- A patient enters her Doctor's consulting room. Neither the doctor, nor the patient, realizes that the door is ajar, instead of being properly closed. The patient is given a cancer diagnosis and the entire waiting room hears both the diagnosis and the patient's distressed response through the partially open door. This is a fictitious example, but these kinds of breaches do happen in health care (Scott *et al.*, 2007). This is a breach of non-digital *information security* i.e. confidentiality has been lost.
- An employee works on a confidential contract on his home computer. He then connects to the company's server from home so that he can deposit it in the shared drive for his boss to read the following morning. He forgets to use the company's Virtual Private Network when making the connection. A hacker is sniffing the network traffic and is able to obtain the details of the contract. This is a breach of *information security* ***and*** *cyber security* i.e. confidentiality has been lost, *and the Internet enabled it.*

These definitions treat cyber security as a subset of information security, and cyber security governance a subset of information security governance. Von Solms and Von Solms also make it clear that the related concepts, such as cyber crime, cyber safety and cyber harm, fall outside the remit of organizational information and cyber security governance.

Having laid the foundations, we can now make the argument that IC is also a cyber security governance concern.

3. Positioning Intellectual Capital (IC)

What is IC composed of? Choong (2008) explains that IC "*is the result of the network effect of utilizing various intellectual, human, capital and organizational resources*." [p.616]. Choong carried out an exhaustive review of definitions and terminologies that are used by researchers to delineate and refer to intellectual capital. He points out, and demonstrates, that many use the term "intangible assets" (IAs) as a synonym for IC. His investigation concluded that there is general consensus that the essence of IC can be captured by a "*three-grouped framework*" [p. 622] which includes (1) human capital, (2) structural capital, and (3) relational capital, but he also makes the case for augmenting this with intellectual property (IP), citing Marr and Schiuma (2001) to argue for its inclusion. Rastogi (2002) offers a different perspective, referring to IC as an organization's "*knowledge management nexus*" (KMN) being formed of a dense dynamic nexus of (1) social capital, (2) human capital and (3) knowledge management.

Some authors refer to '*social* capital', and others use the term '*relational* capital'. Hussinki *et al.* (2017) use the composite term: 'social capital/relational capital'. Hence we will use the terms interchangeably to reflect the part of IC that is related to connections between people and organizations that make up part of the organization's IC.

Wiig (1997) provides some clarifications of the key terms. Human capital, he says, is related to the capabilities and competencies of the employees, whereas structural capital is "*what is left when employees have gone for the night*" [p. 401], i.e. the codified parts of IC. Relational capital, Kale *et al.* (2000) [p. 217] explain, is "*based on mutual trust and interaction at the individual level between alliance partners [and] creates a basis for learning and know-how transfer across the exchange interface.*"

Reed *et al.*, (2006) explain that the different components of IC are co- and inter-dependent, in terms of contributing to the organization's financial performance – a deficiency in one weakens the organization's IC's potential to contribute to the organization's success. In other words, all the individual nodes of the network (the knowledge and experiences of individuals) and the network itself (relationships and organizational structure) need to be preserved and secured for IC to contribute towards organizational success. This confirms Rastogi's (2002) conceptualization of IC as a dynamic inter-related *nexus*.

Some researchers have sought to define IC rather than describe its constituent parts. In 1996, Edvinsson and Sullivan referred to IC as "*knowledge that can be converted into value*" [p. 358]. More recently, in 2016, Dumay defined IC as "*the sum of everything everybody in a company knows that gives it a competitive edge […] Intellectual Capital is intellectual material, knowledge, experience, intellectual property, information […] that can be put to use to create [value].*" [p. 169]. Finally, in 2018, De Santis and Presti defined IC as "*the sum of everything everybody in a company knows that gives it a competitive edge.*"

To summarize: the human capital part of IC reflects its employees' competencies and knowledge (the intellect). This knowledge is sometimes codified, and this process and outcome makes up the structural component of IC. The relational part of IC could be considered the *lubricant* that makes everything interact properly: connecting constituent parts of an organization's IC to ensure that the organization can benefit maximally from their human capital.

There is a strong *knowledge* theme running through this discussion; IC can almost be seen as a galaxy of concepts orbiting the core of knowledge held by the employees within an organization. Yet it is also an "intangible asset" (Choong, 2008; Pike *et al.*, 2005). This very intangibility might lead to an assumption that its security is not a cyber-related board concern. However, if we examine the IC concept more closely, a compelling argument for including responsibility for its preservation under the cyber security governance

umbrella emerges.

3.1. Intellectual Capital: Cyber Dimensions and Concerns

In this section, we will argue for two distinct dimensions of IC that are relevant to our cyber discussion, and explain how cyber security governance is a cross-cutting IC concern.

3.1.1. Knowledge: The First Dimension

The word "know" and "knowledge" is a strong theme in definitions and elucidations of IC, as illustrated in the previous section. A definition of knowledge helps us to make some interesting connections:

> **Knowledge** is defined by (Davenport and Prisak, 1998)[p. 5]: "*a fluid mix of framed experience, contextual information, values and expert insight that provides a framework for evaluating and incorporating new experiences and information. It originates and is applied in the minds of knowers. In organizations, it often becomes embedded not only in documents, or repositories, but also in organizational routines, processes, practices and norms.*"

This conceptualization of knowledge is reminiscent of Choong's mention of IC's *network effect* and Rastogi's *nexus* conceptualization of IC. Indeed, Dumay uses the word "knowledge" in his IC definition, as do De Santis and Presti (2018). Other researchers also emphasize the "knowledge" or "knowing" aspects of IC (Nahapiet and Ghoshal, 1998; Edvinsson and Sullivan, 1996).

Shedden *et al.* (2010) suggest that three different kinds of knowledge can be distinguished: (1) distributed knowledge (held collectively), (2) tacit knowledge held by individuals, and (3) explicit knowledge held by individuals. We can draw some parallels here with Choong's IC's components: the first aligns with *relational* capital, the second with *human* capital, and the third with *structural* capital. Hsu and Sabherwal (2011) also argue that the three components of IC (as enumerated by Choong, 2008) align with the three different kinds knowledge.

Nahapiet and Ghoshal (1998) refer to the value of the resources that the organization gains access to via the network of relationships their human capital agents have established: the relational-capital related knowledge. Inkinen (2015) report that the organization's performance is enhanced primarily via its "*interactions, combinations and mediations*" [p. 518]. De Santis and Presti (2018) considers much organizational knowledge to be embedded within these relationships. Bueno *et al.* (2004) argue that the knowledge sharing that happens due to these relationships generates a competitive advantage.

Knowledge can, of course, be either explicit (codified) or tacit (not recorded anywhere) (Nahapiet and Ghoshal, 1998). Shedden *et al.* (2010) explain that even if tacit knowledge *can* be recorded, it can usually only be understood by someone with the requisite level of tacit knowledge to make sense of it. Shedden *et al.* carried out an investigation at a company and discovered that even if it were possible to document a particular process, i.e. make it explicit, the process failed if certain key people were not present. They also found that some tacit knowledge was very hard for people to articulate due to the "messy complexity" of the knowledge and their engagement with particular processes and practices. This surely mirrors the interconnected and interdependent nature of the IC of an organization.

IC is strongly rooted in oft intangible knowledge, as opposed to being merely a networked collection of facts and descriptors. Such knowledge should be preserved and protected. Knowledge, then, is the *first* governance dimension of IC.

3.1.2. Information: The Second Dimension

Dumay (2016) also uses the word "information" in his definition of IC. It is thus useful to provide a definition

of information:

> **Information** is defined by (Losee, 1997) [p. 254] as: "*the characteristics of the output of a process, these being informative about the process and the input*." In other words, information can be thought of as a set of descriptors or facts.

Recall that knowledge can either be tacit (in people's minds) or explicit: codified in some way. Such codified knowledge has information properties, since some kind of process was engaged in to code the knowledge. Wiig's (1997) elucidation of the structural capital IC component suggests that this is where codified knowledge is stored as information, and we can expect this information to be stored digitally in this day and age.

IC is not, therefore, merely a synonym for a *knowledge* network: it is a much more complex entity. IC contains both knowledge, relational and informational aspects. It is made up of a complex network of different entities, some tangible, and others intangible; some knowledge-based, others information-based and others being grounded in the relationships between employees and the trust the employees have in the organization itself.

We now provide two examples of IC-related information. As the *first*, consider that many organizations use data mining techniques to reveal patterns and insights in their stored information. This then constitutes new organizational knowledge. Consider that such information could be stolen, and that equally powerful data mining techniques could be used by a competitor to reveal the hidden knowledge. In this case, too, a loss of information constitutes a potential loss of new organizational knowledge i.e. part of the organization's structural IC.

Secondly, consider that organizations often engage in activities to measure their IC. IC measurements usually result in reports that are communicated to stakeholders (Edvinsson, 1997; Bontis, 2001). Such reports can be considered to be information, since they align with Losee's definition (provided above) as being an output of a process, describing its inputs. The securing of these reports is also a general IC security governance concern.

It is clear that some IC will be codified and stored as information. Such information should be preserved and protected. IC thus also has an *information* governance dimension.

3.2. Cyber Security Governance: A Cross-Cutting Concern

Recollecting the cyber-related definition provided in Section 2, we conclude that, if the Internet is involved in the storage or transmission of any part of IC, preservation thereof becomes a cyber security governance concern. It is obvious that the informational components of IC can be stored and transmitted digitally, so there is no doubt that cyber security governance is required to preserve and secure these components.

What about knowledge? Knowledge is no use to an organization unless it is applied to solve problems, and employees will often meet and engage in discussions to do so. Now, consider the fact that we are surrounded by Internet-enabled devices that record what we are saying, and cameras that record what we do. Knowledge, in this case, can leak without the knowledge holders even being aware of it. Moreover, it is entirely possible that a malicious employee will steal knowledge via an Internet-connected device, the loss of which will harm the organization (Harvey and Lusch, 1997). Hence, the preservation of IC-related knowledge is also a cyber security governance concern.

Ilvonen *et al.* (2018) enumerate four kinds of knowledge risks: knowledge loss, spillover (a competitor gets hold of it), theft and misappropriation (an organization's failure to patent their knowledge assets). We use these categories in our examples below to clarify differences.

Consider the following examples to clarify the impact of this section's arguments:

1. Non-Cyber:

- *Knowledge loss:* a key employee retires. It is discovered, after she leaves, that she is the only person who knows how to make a particular legacy system work. This system is critical to business processes, so the organization rehires the retiree to train another knowledge worker[1]. IC was unwittingly lost when the person retired. This is not a cyber security issue. It is an IC-related *knowledge* security governance issue.
- *Indirect knowledge spillover:* an employee (let us call him John) leaves an organization and goes to work for a competitor. He takes a copy of the organization's logged IT incidents database with him. His new employer uses data mining to interpret the data and find clear patterns to suggest that the organization's infrastructure has severe IT issues, which weaken their competitive ability. The new employer has used that information to construct knowledge, but the original breach was an *information* security breach, not an IC-related knowledge breach, and not a cyber security governance issue.
- *Knowledge spillover:* two employees go to a local coffee bar and start to "talk shop". They do not realize that a competitor's employee is overhearing their discussion. This is an IC-related *knowledge* security governance issue, because the Internet did not enable the leakage of the knowledge. A similar example is related to John (from the previous example), who has knowledge of confidential relationships that have been very valuable to the organization. His leaving constitutes a knowledge loss that could lead to spillover, but this is not a cyber security governance concern. He has merely taken the intangible knowledge with him, so that the knowledge is no longer an organizational IC asset.

2. Cyber-enabled:
   - *Knowledge theft and misappropriation*: an employee becomes disgruntled. She covertly records confidential meetings she attends, and uploads the recordings to her Dropbox account from her Smartphone. She then sells these recordings to a competitor, who utilizes this knowledge. This is a fictitious example, but there are many real-life examples of this kind of scenario (Hopping, 2013). IC is leaked, and the Internet enables it. This is an IC-related *cyber* security concern because the Internet enabled the theft.
   - *Knowledge loss*: a group of highly knowledgeable employees is trying to solve a problem. One employee's smartphone has a voice-enabled help feature, which is recording everything they say, without anyone being aware of this. Employees in the company providing the service listen to the recordings. This is, once again, a fictitious scenario, but is not outside the realms of possibility (Cook, 2019). In this kind of scenario, IC knowledge is leaked and the Internet enabled it, making it an IC-related *cyber* security concern.
   - *Knowledge theft*: an external company is brought in to help an organization to measure their IC. They write a report, which is held on their own server – but they do not encrypt it. Cyber criminals breach their systems and gain access to the reports. The organization whose IC reports have been leaked have been unable to control the disclosure of their IC and their IC is damaged by the breach. This makes it a *cyber*-related IC security issue.

These examples suggest that while much IC knowledge resides in employee minds, and is intangible (the human capital part of IC), even this knowledge can be leaked via the Internet. Information artifacts of IC also need to be secured. They, too, can be leaked via the Internet if they are insecurely stored or transmitted, or stolen, as demonstrated by the examples given above. We can thus conclude that the securing of both information and knowledge dimensions of IC are cyber security governance concerns.

4. IC Security

[1] https://en.wikipedia.org/wiki/Grace_Hopper (The organization was the US Navy and the employee was Grace Hopper).

We have argued that IC is a knowledge-related concept and that knowledge and information, while related, are distinctly different concepts. Hence, in securing IC, we need to consider how IC-related knowledge should be secured, while benefiting from established information security measures for the informational components of IC. To consider the securing of knowledge aspects we consider *knowledge security* concepts, which Ilvonen (2013) [p. 152] defines as:

> "*the process of making and keeping the knowledge of people working at a company secure*."

From this, it then follows that **knowledge security governance** can be described as:

> "*the governance of knowledge security, regardless of its format*."

Desouza (2006) argues that knowledge security is required because (1) knowledge gives the organization a competitive advantage, (2) it takes a long time and a great deal of effort to develop, and, (3) if lost, is non-trivial to replace. He points to a number of challenges in securing knowledge, including its intangibility, its fluidity, its dynamic nature and its mobility. All these characteristics also make the knowledge dimensions of IC challenging to capture and secure.

The definitions we have provided of knowledge security are perhaps as imprecise as some definitions of other kinds of security concepts. However, the aim of this paper is to provide clarity to BoDs, so we need to convert this somewhat philosophical discussion into actions that BoDs can take, in terms of securing their IC. An essential first step in securing IC is to delineate all IC assets, and we discuss this activity before proceeding to consider actions related to governing the security thereof.

4.1. Step 1: Delineating IC Assets

We have argued that IC is a knowledge-related concept, and that knowledge is essentially an asset (Ilvonen, 2013). As such, we plan to follow Shedden *et al.'s* (2010) recommendation that organizations identify their critical knowledge. This advice is echoed by Shamala *et al.* (2014) and Elson *et al.* (2006). They also highlight the need to pinpoint where leakage of such knowledge could occur.

If we consider how this applies to the IC domain, M'Pherson and Pike's (2001) suggest that all aspects of IC be measured, so that it can be managed effectively. This mirrors the activities routinely engaged in when it comes to the organization's information assets and the security thereof (Posthumus and Von Solms, 2004). Ordóñez de Pablos (2003) argues that the action of measuring and reporting IC gives companies a competitive advantage and Roos and Roos (1997) argue that keeping track of an organization's IC helps to predict its future performance. These activities can help an organization to come to grips with the extent of their IC footprint, both cyber and otherwise.

It is clearly going to be challenging to record the full extent of an organization's IC, given that human knowledge and information assets related to IC have to be included. Despite the challenges of delineating an organization's IC, it is not something that can be neglected. Unless the organization has some idea of where its IC resides, and how and whether it is codified, they will never know when and how they have lost it, or how to secure it. Monitoring their most valuable asset is surely a governance concern.

A full discussion of exactly how to measure the IC asset is out of context for this paper. We thus direct those wishing to carry out this step to the existing literature related to information asset recording (Posthumus and Von Solms, 2004; Laney, 2017) and the existing literature related to measuring IC assets (Kianto *et al.*, 2018; Jordão and Almeida, 2017; Chen *et al.,* 2014; Pedrini, 2007).

We next consider *how* IC security ought to be governed, while being sensitive to its hybrid nature.

4.2.Step 2: Governing IC Security

Having concluded that IC security requires information and knowledge governance, we now consider exactly how IC ought to be secured and governed. The fields of information security and cyber security governance have received a great deal of attention. Consider that 82 of the world's 195 countries have cyber security strategy policies[2], reflecting the global concern around information and cyber security, and relative maturity of good practice in these domains. We can benefit from their insights but, when it comes to knowledge-based governance approaches, there is a need to formulate good practice to augment these approaches.

Desouza and Vanapalli (2005) suggest that efforts to secure knowledge should occur at three levels, and, because IC is knowledge-based, these can inform our approach: (1) the product, (2) the process and (3) the people. The *product* is the tangible part of IC i.e. explicit knowledge that is held in digital or other concrete format. The *process* is arguably Choong's structural component of IC and Rastogi's "knowledge management". *The people* mirror Choong's human and relational components of IC and a large chunk of IC is linked to the knowledge and abilities of the humans within the organization (Edvinsson, 1997; Bontis, 2001; Mayo, 2000; Su, 2014).

An example of a *product* is the reports generated based on measurements of IC, which is information, according to Losee's (1997) definition. Another example is the codified explicit knowledge of employees within the organization. In the securing of these information-based IC components, all three aspects of *information* security apply: confidentiality, integrity and availability of the information (Desouza, 2006). In the first place, the organization has to retain control over the extent of IC report disclosures (Baughn *et al*., 1997; Mohamed *et al.,* 2006; Laperche, 2018), in much the same way as it controls disclosure of its other information assets. This is arguably a ***confidentiality*** concern. The need for IC reports to be "reliable and responsible" speaks to the need for information ***integrity*** (CIC, 2008). This also becomes a cyber security governance concern if information is transmitted via the Internet. Jennex and Zyngier (2007) argue for the need for the organization to ensure that codified knowledge is *recent* and *comprehensive*, which again reflects the need for ***integrity***. If any such IC-related information is stored digitally, a malware attack could also compromise its ***availability***.

The increase in economic espionage (Martemucci, 2015; Department of Justice, 2019) is another potential ***confidentiality*** risk. Nasheri (2012) argues that the proliferation of cyber-enabled espionage is being exacerbated by the increasing number of Internet-enabled devices diffusing across society. These all extend the attack surface that can be targeted by those wishing to steal organizations' valuable IC assets.

Securing the *process* is related to the organization's need to be able to search for and retrieve relevant codified knowledge when required (Jennex and Zyngier, 2007). This parallels the ***availability*** concerns of traditional information security, as does Jennex and Zyngier's (2007) third risk: *the risk of the right people not getting the knowledge needed to make decisions*. Desouza and Vanapalli (2005) also talk about the risk of *unauthorized access*. This parallels the need to preserve the ***confidentiality*** of codified knowledge. Johanson *et al.* (2006) cite concerns about organizations inadvertently revealing company secrets, which could compromise their competitive advantage, confirming the confidentiality concern.

A "security knowledge" approach to *people*-related IC would need to commence by identifying the key people whose knowledge is tacit, unarticulated and essential in making particular organizational processes work. The challenge in securing this aspect lies in working out how to encourage knowledge sharing (Su, 2014; Wang *et al.,* 2014) while protecting such knowledge from those outside the organization. This aligns with Lundgren and Möller's (2019) formulation of information security that focuses on these same tensions i.e. balancing

[2] http://cyberlawcybersecurity.com/cyber-security/cyber-security-laws-different-countries/

confidentiality and sharing so that both parties benefit while both retain control over their knowledge assets.

The other 'people' aspect is related to the relationships between human agents, both in and outside the organization. It is going to be challenging to make these tangible, and, even if a snapshot could be taken for the purposes of IC measurement, it is going to be difficult to keep this up to date. It might be better to follow the approach mentioned in the previous paragraph, of identifying the organization's well-connected individuals.

The outcome of the previous discussion is depicted in Figure 1, which includes the "knowledge security" threats cited by Ilvonen (2013, 2018). There are three broad categories of knowledge-specific threats: (1) leaks to competitors (i.e. knowledge spillover/misappropriation), and intentional harm (i.e. knowledge theft) threatening confidentiality, (2) employee turnover threatening availability of knowledge held by that employee (i.e. knowledge loss), and (3) obsolete or inaccurate knowledge, which threatens the integrity of the knowledge and could lead to uninformed and faulty decisions.

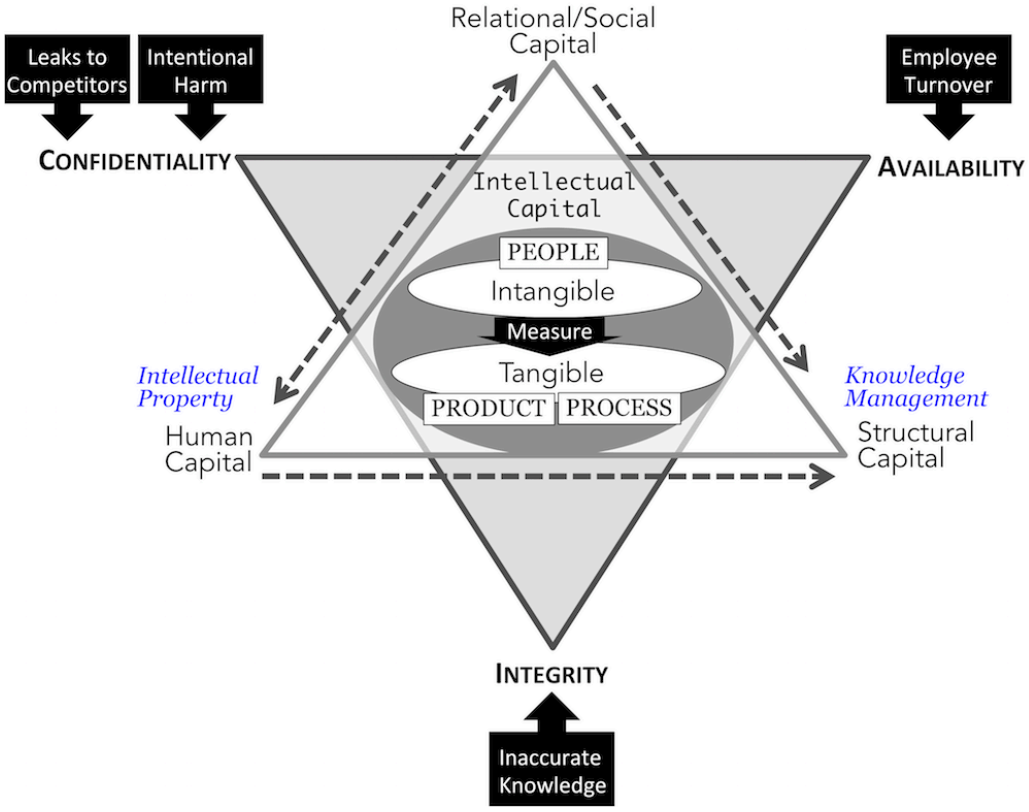

Figure 1: Summarizing IC Concepts and showing Knowledge-Specific Threats

4.3. Bringing it all together

Based on this discussion, Figure 2 depicts the relationships between information security, cyber security, knowledge security, and other cyber space concerns. IC is included, as a concern that spans *knowledge security, information security* and *cyber security*.

The previous discussion makes it clear that IC security requires elements of *information* security governance, *knowledge* security governance and *cyber* security governance, as shown in Figure 3.

We are now ready to define IC cyber security governance. We can benefit, once again, from existing definitions. Intellectual Capital Management (ICM) focuses on "*building and governing intellectual assets from strategic and enterprise governance perspectives with some focus on tactics.*" (Wiig, 1997) [p. 400]. Secundo *et al.*

(2017) argue that the value that IC creates in an organization is directly dependent on the organization's ability to manage its IC.

IC cyber security governance requires the delineation of IC assets as a pre-requisite, and can be defined as:

> "*the governance of information security for tangible knowledge-related artifacts, and knowledge security for its intangible components, utilizing cyber security governance measures.*"

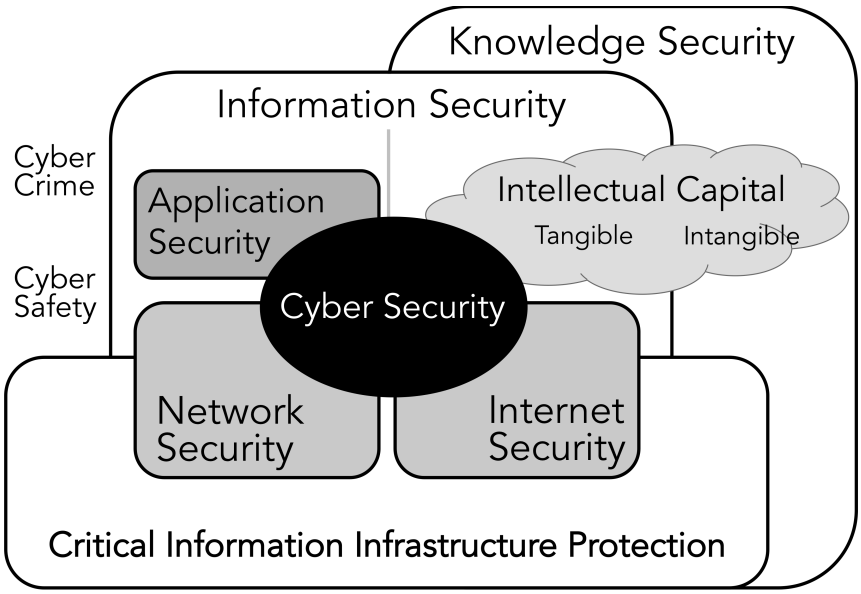

Figure 2: Extending Figure 2 from Von Solms & Von Solms (2018) to show how Intellectual Capital fits in i.e. spanning information, knowledge and cyber security.

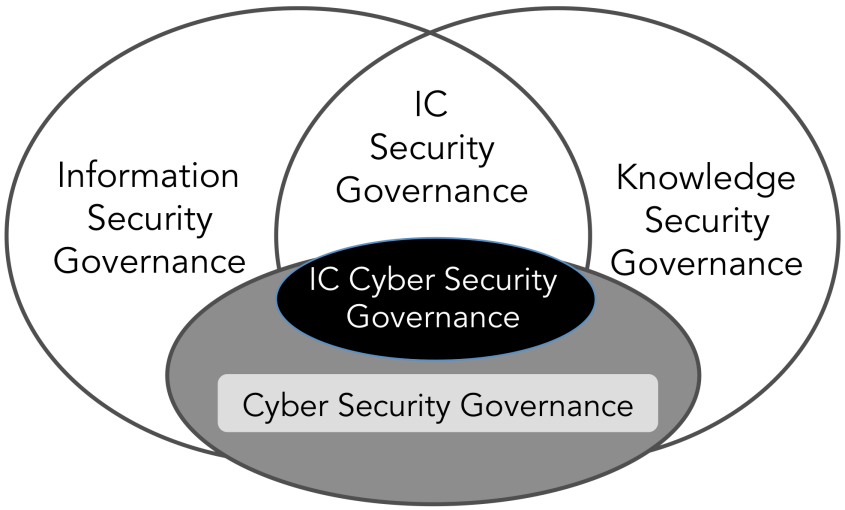

Figure 3: Different Governance Types, and their Interdependencies

5. IC Security Governance: Simplifying and Clarifying

The governance of information is important to modern-day enterprises. "Cyber security governance" has also become critical (Von Solms and Von Solms, 2018), calling for the direct attention and oversight of BoDs and executive management teams (AIG, 2019). We have situated IC security governance within the cyber governance space too, and plan to highlight BoDs' responsibilities in this respect.

The goal of this paper is to argue that BoDs should be mobilized towards the effective governance of IC security. Scully (2014) argues that boards are responsible for the cyber security of the enterprise. We argue that the cyber-related governance of IC should also be included in this mandate. BoDs and executive management teams must pay more attention to the potential negative effects of cyber attacks (Von Solms and Von Solms, 2006) and we now argue that IC could also be impacted. It would certainly be negligent not to consider these negative effects (see Gigante (2019) for statistics related to cyber attacks since 2008). That being so, BoDs need to know exactly what governing cyber security entails, in this day and age.

We first explain how to communicate the message to BoDs, and then provide an outline of advisable actions in this respect.

5.1. Formulating the Message

Von Solms and Von Solms (2018, p.8) recommend that, when confronting boards with cyber security risks threatening the welfare of the enterprise, the person presenting the message ought to:

(1) concentrate primarily on the risks arising from the organization's cyber space engagement,
(2) make the consequences of *not* addressing those risks, from a legal and brand-name angle, salient, and
(3) emphasize the risks for any new systems; since this would increase the enterprise's presence in, and dependence on, cyber space even further.

Based on these assertions, and the arguments earlier in this paper, we summarize the message that CIOs and information security managers need to hear, with respect to IC security governance, as follows (Figure 4):

1. *BoDs are responsible and accountable for organizational welfare* (argued in the Introduction, citing Hall *et al.* (2007), confirmed by Flowerday and Von Solms, 2005).
2. *Businesses are increasingly reliant on the Internet* (Ng and Tsui, 2010). The affordances of cyber space have brought great advantages, in terms of convenience, scalability and cost effectiveness (as argued in the introduction, citing Goel and Sunena (2018) and Sukhodolov *et al.* (2018)).
3. This relationship, while delivering great benefit (Francis, 2019), also *exposes the organization to attendant risks* (Carabott, 2011), because the cyber criminal's attack surface is enlarged, especially as new systems come on board (derived from Von Solms and Von Solms' (2018, p.8) first and third recommendations).
4. *The welfare of the organization is thus highly dependent on the health of this cyber relationship* (derived from first recommendation from Von Solms and Von Solms (2018, p.8) and from Uretsky (2002)).
5. *IC can be damaged by the actions of cyber criminals or malicious insiders*, which threaten the confidentiality, integrity and availability of the organization's knowledge or knowledge artifacts that are stored or transmitted via cyber space (Solove and Citron, 2017) (extended from Von Solms and Von Solms' (2018, p.8) second recommendation),
6. *IC security requires cyber security governance* (argued in Section 4).
7. ***BoDs are responsible and accountable for IC-related cyber-security governance***, which includes protecting IC from the activities of cyber criminals (Trautman and Ormerod, 2016; Price, 2017; Islam and Stafford, 2017).

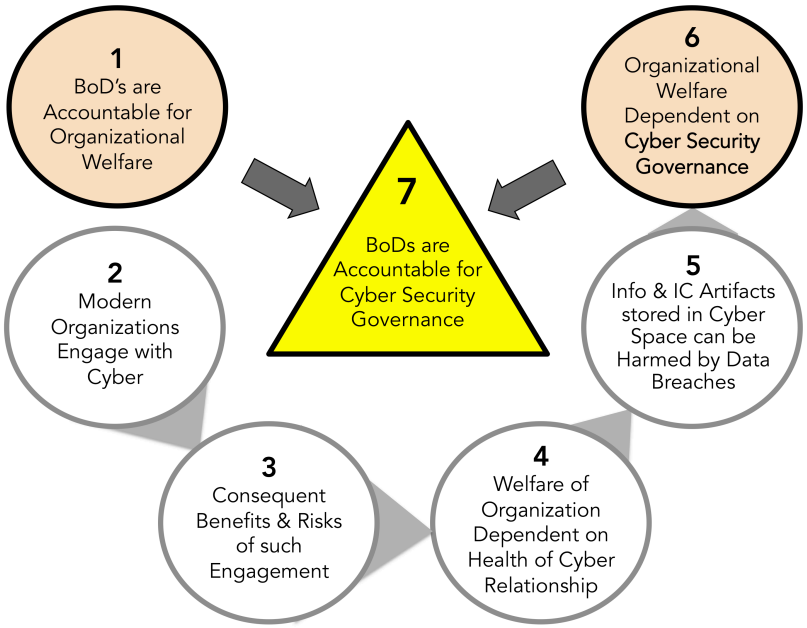

Figure 4: Arguments leading to the conclusion that BoDs are responsible and accountable for cyber security governance.

With this argument, we advocate re-directing the IC 'security message' to boards, and basing it firmly on cyber threats. This does not necessarily suggest that activities and systems 'not linked to cyber space' can be ignored. We suggest that the time available to interact with BoDs should be used as productively as possible – to garner the support and engagement of board members.

Highlighting and focusing on cyber security risks, as opposed to the more comprehensive and general information security risks, would definitely make it easier for boards to evaluate their accountabilities and responsibilities with respect to IC security as well as other cyber security aspects.

5.2. Translating "Should" to "How to"

BoDs must insist on being informed and made aware of the enterprise's involvement in, and exposure to, cyber space (Von Solms and Von Solms, 2018). They should understand that even something as seemingly nebulous as IC can be lost or compromised, and that this could damage the future potential of the organization.

These aspects should feature as permanent BoD agenda items, assisting BoDs in properly governing their organization's IC-related cyber risks. The elucidation of the links between IC security and the other kinds of security serve to place it within the realms of cyber security governance.

We do not seek to be completely prescriptive of all the actions that BoDs should take, since our focus is primarily on ensuring the lucidity and understandability of the message to BoDs and executive teams. Here we flesh out Von Solms and Von Solms' (2018) broad brush recommendations, with respect to cyber security governance. We also include IC-related cyber security governance recommendations.

Weill and Ross (2004) propose a corporate and asset governance framework. The framework depicts IT governance mechanisms being connected to "Information and IT assets", but their framework does not depict the role of cyber security governance. A number of IC-related constructs appear in their framework, including human assets, IP assets and relationship assets. Von Solms and Von Solms (2018) argued that cyber security governance is required when information is stored or transmitted via the Internet. We have also argued that the securing of IC has a cyber security governance dimension.

We now suggest some actions that can be undertaken by BoDs to embrace all their cyber-related governance responsibilities, using similar questions as applied to the cyber security governance domain, in order to ensure that board members understand the associated risks of their cyber exposure to both tangible information and intangible knowledge i.e. IC-relevant components, adapting the questions that Weill and Ross (2004) pose related to effective *IT governance*:

(1) *What decisions must be made to ensure effective cyber governance of information and IC, and who makes these decisions?*

a. Consider including a cyber expert on the board (Post, 2014; Dickstein, 2015; Price, 2017; Scholl, 2017; Carr, 2014; Rai, 2014; Trautman *et al.*, 2013).

b. Establish an affiliated BoD committee that has responsibility for overseeing and understanding the organization's cyber security state of play, and who can report to the board. Their responsibilities are to ensure that the following is carried out:

i. Identification of all organizational assets, both tangible (Posthumus and Von Solms, 2004) and intangible i.e. IC (Stewarts and Ruckdeschel, 1998). This should include a prioritization of the assets in order to decide which risks to manage, which to avoid and which to outsource (Dickstein, 2015; McLaughlin, 2016; Price, 2017; Scholl, 2017; Veltsos, 2015; Carr, 2014; Rai, 2014). It is especially important to re-engage regularly with this step, especially as new knowledge-based systems come into play in the organization, or after each IC measurement exercise.

ii. Monitoring of the cyberspace for new risks (both information- and knowledge-related) and to monitor physical risks (Stark and Fontaine, 2015). This should include considering how knowledge can be leaked or maliciously altered (i.e. knowledge loss/theft/spillover/misappropriation threats (Ilvonen *et al.*, 2018)).

iii. Deciding which standard cyber security mechanisms will be used to secure organizational information and knowledge (Jennex and Zyngier, 2007). A specific security framework, such as NIST's Cybersecurity Framework[3] (CSF), might be adopted. A number of frameworks could be investigated by the cyber committee and recommendations made to the board for approval.

iv. Monitoring of the organization's IC-cyber-related knowledge security (Ilvonen, 2013), and improve measures, if required, to address Internet-enabled knowledge leakage, and compromise of knowledge integrity.

v. Deciding on actions that should be undertaken pro-actively to detect intrusions (Veltsos, 2015; Stark and Fontaine, 2015) and attempts to steal or compromise knowledge assets (Desouza and Vanapalli, 2005) – addressing the knowledge leakage threat. These could include malicious actions (intentional harm threat) or mistakes (made by internal or external actors) leading to knowledge loss (Carr, 2014).

c. Consider retaining consultants to evaluate the organization's current cyber risk governance mechanisms (Post, 2014; Dickstein, 2015). These could advise and feed into the cyber committee's deliberations.

[3] https://www.nist.gov/cyberframework

d. Consider retaining a lawyer or contracting one to outline the legal implications of the risks (Scholl, 2017; Stark and Fontaine, 2015; Rai, 2014).

e. The board should also consider authorizing and paying for an annual penetration test by ethical hackers (Stark and Fontaine, 2015). Depending on the size of the organization, consider offering a bounty to hackers for finding vulnerabilities in the organization's cyber infrastructure (Price, 2017).

f. Instruct responsible bodies to formulate plans of action to address the risks, and refresh these annually:

    i. *A plan to direct responses and actions, should a breach occur* (Dickstein, 2015; McLaughlin, 2016; Price, 2017; Carr, 2014; Stark and Fontaine, 2015). Dickstein also recommends appointing a rapid response team. Consider retaining an expert company to assist in responding and recovering when a cyber breach occurs (Stark and Fontaine, 2015). After recovering from a breach, engage in a "lessons learned" session after mop up operations have concluded (Stark and Fontaine, 2015). The latter "knowledge" also needs to be treated as confidential and merits security-related attention to ensure that its CIA properties are assured i.e. knowledge theft and obsolescence threats are managed.

    ii. *A business continuity plan* to be implemented in the event of a natural disaster or cyber attack occurring (Stark and Fontaine, 2015). Consider taking out cyber insurance (Post, 2014; Dickstein, 2015; Stark and Fontaine, 2015; Trautman and Altenbaumer-Price, 2010).

    iii. *A plan to recruit and retain cyber talent* (Price, 2017) – addressing the employee turnover "knowledge loss" risk.

(2) How will these decisions be made and monitored?

a. Reports from the cyber committee should be a permanent agenda item to ensure that the board stays informed about the current cyber security state of play (Veltsos, 2015).

b. Ensure that the organization is spending adequately on cyber security (Veltsos, 2015; Stark and Fontaine, 2015; Rai, 2014), but require such spending to be justified, in terms of the risk that is being mitigated (Veltsos, 2015) and the value of the protected asset, both tangible and intangible.

c. Oversee execution of plans of action. Where plans have been formulated, assign a board member to oversee each one, and to act as a board liaison to report on progress or to request and justify more resources if required.

d. Due Diligence: stakeholder security practice:

    i. *Monitor* the cyber security culture within the organization, to ensure that the organization's employees understand that cyber security is not only a technology issue (Post, 2014; McLaughlin, 2016; Scholl, 2017; Stark and Fontaine, 2015; Rai, 2014). Direct that regular awareness raising and training sessions be conducted within the organization (Post, 2014; Carr, 2014; Stark and Fontaine, 2015).

    ii. *Require reports* from the organization's vendors (including software vendors) to ensure that their cyber and information security governance measures are adequate to protect this organization's data (Post, 2014; Dickstein, 2015; Price, 2017; Stark and Fontaine, 2015).

iii. If external contractors are brought in to measure IC, ensure that they provide evidence that their reports are stored securely within that organization's cyber space, and communicated securely to this board's members and other authorized stakeholders (Dickstein, 2015). This can help to prevent knowledge leakage.

6. Conclusion

BoDs and executive management teams are responsible and accountable for the wellbeing of any modern organization. Since most, if not all, organizations are dependent on their IC, securing IC plays a critical role in ensuring the well-being of such an organization. Most organizations, worldwide, utilize cyber space. BoDs have to take cognizance of this reality and the opportunities this affords cyber criminals to damage the organization's IC.

It is thus important for BoDs to understand what IC security is, how it relates to cyber security, and to be aware of the importance of securing IC. Moreover, they need to understand that the governing of IC-related cyber security is key to their general governance mandate, and crucial to the future welfare of the organization. We have made this argument in this paper, and provided an outline of the actions BoDs need to take to govern their IC's security, as part of the cyber security governance remit.

We hope that BoDs and executive management teams will find this discussion helpful and informative.

Acknowledgements

Please note that the authors have been listed in alphabetical order, to reflect their equal contributions to this paper.

References

Abraham, C., Chatterjee, D. and Sims, R.R. (2019), "Muddling through cybersecurity: Insights from the US healthcare industry", *Business Horizons*. https://doi.org/10.1016/j.bushor.2019.03.010, In Press.

AIG. (2019), "How Boards of Directors Really Feel About Cyber Security", available at: https://www.aig.co.uk/insights/taking-control-of-cyber-risk (Accessed 20 April 2019).

Althonayan, A. and Andronache, A. (2018), "Shifting from Information Security towards a Cybersecurity Paradigm", In *Proceedings of the 2018 10th International Conference on Information Management and Engineering, Salford, U.K.,* pp. 68-79.

Baughn, C.C., Denekamp, J.G., Stevens, J.H. and Osborn, R.N. (1997), "Protecting intellectual capital in international alliances", *Journal of World Business*, Vol. 32 No. 2, pp. 103-117.

Bay Dynamics. (2015), "How Boards of Directors Really Feel About Cyber Security Reports", available at: https://baydynamics.com/resources/how-boards-of-directors-really-feel-about-cyber-security-reports/ (Accessed 20 April 2019).

BBC. (2013), "NHS Surrey fined £200,000 after losing patients' records", 12 July, available at: https://www.bbc.com/news/technology-23286231 (accessed 9 July 2019).

Bianchi, D. and Tosun, O. K. (2019), "Cyber Attacks and Stock Market Activity", available at SSRN: https://ssrn.com/abstract=3190454 or http://dx.doi.org/10.2139/ssrn.3190454

Blair, M. M. and Wallman, S.M. (Eds). (2000), *Unseen wealth: Report of the Brookings task force on intangibles*, Brookings Institution Press, Washington, DC.

Bontis, N. (2001), "Assessing knowledge assets: a review of the models used to measure intellectual capital", *International Journal of Management Reviews*, Vol. 3 No. 1, pp. 41-60.

Bueno, E., Paz Salmador, M. and Rodríguez, Ó. (2004), "The role of social capital in today's economy: empirical evidence and proposal of a new model of intellectual capital", *Journal of Intellectual Capital*, Vol. 5 No. 4, pp. 556-574.

Californians for Consumer Privacy. (2018), "The California Consumer Privacy Act of 2018", available at: https://www.caprivacy.org/ (Accessed: 19 April 2019).

Carabott , E. (2011), “Top 37 Risks Businesses Run with Uncontrolled Internet Usage”, available at: https://techtalk.gfi.com/top-37-risks-admins-uncontrolled-internet-usage/ (Accessed 20 April 2019).

Carr, D. F. (2014), “Cybersecurity: How Involved Should Boards Of Directors Be?”, available at: https://www.informationweek.com/government/cybersecurity/cybersecurity-how-involved-should-boards-of-directors-be/d/d-id/1298127, (Accessed 18 May, 2019).

Chen, J., Zhu, Z. and Yuan Xie, H. (2004), “Measuring intellectual capital: a new model and empirical study”, *Journal of Intellectual Capital*, Vol. 5 No. 1, pp. 195-212.

Choong, Kwee Keong. (2008), “Intellectual capital: definitions, categorization and reporting models”, *Journal of Intellectual Capital*, Vol. 9 No. 4, pp. 609-638.

Cook, J. (2019), “Amazon employees listen in to thousands of customer Alexa recordings”, available at: https://www.telegraph.co.uk/technology/2019/04/11/amazon-employees-listen-thousands-customer-alexa-recordings/ (Accessed 23 May 2019).

CIC. (2008), “EFFAS Commission of Intellectual Capital Principles for Effective Communication of Intellectual Capital”, available at: https://effas.net/pdf/setter/EFFAS-CIC.pdf (Accessed 11 April, 2019).

Department of Justice. (2019), “Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE’s Trade Secrets”, 23 April, available at https://www.justice.gov/opa/pr/former-ge-engineer-and-chinese-businessman-charged-economic-espionage-and-theft-ge-s-trade (Accessed 6 July, 2019).

De Santis, F. and Presti, C. (2018), “The relationship between intellectual capital and big data: a review”, *Meditari Accountancy Research*, Vol. 26 No. 3, pp. 361-380.

Desouza, K.C. (2006), “Knowledge Security: An Interesting Research Space”, *Journal of Information Science & Technology*, Vol. 3 No. 1, pp. 1-7.

Desouza, K.C. and Vanapalli, G.K. (2005), “Securing knowledge in organizations: lessons from the defense and intelligence sectors”, *International Journal of Information Management*, Vol. 25 No. 1, pp. 85-98.

Dierickx, I. and Cool, K. (1989), “Asset stock accumulation and sustainability of competitive advantage”, *Management Science*, Vol. 35 No. 12, pp. 1504-1511.

Dickstein, Michael. (2015), “Cybersecurity: The Board's Role”, available at: https://www.spencerstuart.com/research-and-insight/cybersecurity (Accessed 18 May 2019).

Dumay, J. (2016), “A critical reflection on the future of intellectual capital: from reporting to disclosure”. *Journal of Intellectual Capital*, Vol. 17 No. 1, pp. 168-184.

Edvinsson, L. and Sullivan, P. (1996), “Developing a model for managing intellectual capital”, *European Management Journal*, Vol. 14 No. 4, pp. 356-364.

Edvinsson, L. (1997), “Developing intellectual capital at Skandia”, *Long Range Planning*, Vol. 30 No. 3, pp. 366-373.

Elson, R.J. and LeClerc, R. (2006), “Customer information: protecting the organization’s most critical asset from misappropriation and identity theft”, *Journal of Information Privacy and Security*, Vol. 2 No. 1, pp. 3-15.

EU Parliament. (2018), “Home Page of EU GDPR,” available at: https://www.eugdpr.org/(Accessed 12 April 2019).

Flyverbom, M., Deibert, R. and Matten, D. (2019), “The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business”, *Business & Society*, Vol. 58 No. 1, pp. 3-19.

Flowerday, S. and Von Solms, R. (2005), “Continuous auditing: verifying information integrity and providing assurances for financial reports”, *Computer Fraud & Security*, Vol. 2005 No. 7, pp. 12-16.

Francis, K. A. (2019), “How Has the Internet Impacted Businesses?” available at: https://smallbusiness.chron.com/internet-impacted-businesses-321.html (Accessed 20 April 2019).

Gigante, A. (2019), “Breached data: stats and graphical representation (haveibeenpwned source)”, available at: https://medium.com/@andrea.gigante/breached-data-stats-and-graphical-representation-haveibeenpwned-source-1ce78720432f (Accessed 20 April 2019).

Goel, M.S. and Sunena, M. (2018), “Role of Information and Communication Technology in the survival of small business”, *International Journal of Research*, Vol. 5 No. 4, pp. 3038-3042.

Hall, A.T., Bowen, M.G., Ferris, G.R., Royle, M.T. and Fitzgibbons, D.E. (2007), "The accountability lens: A new way to view management issues", *Business Horizons*, Vol. 50 No. 5, pp. 405-413.

Harvey, M. and Lusch, R. (1997), "Protecting the core competencies of a company: intangible asset security", *European Management Journal*, Vol. 15 No. 4, pp. 370-380.

Hopping, Clare. (2013), "How to protect your company from leaked trade secrets", https://www.itpro.co.uk/strategy/20833/how-protect-your-company-leaked-trade-secrets (Accessed 23 May 2019).

Hsu, I.C. and Sabherwal, R. (2011), "From intellectual capital to firm performance: the mediating role of knowledge management capabilities", *IEEE Transactions on Engineering Management*, Vol. 58 No. 4, pp. 626-642.

Hussinki, H., Ritala, P., Vanhala, M. and Kianto, A. (2017), "Intellectual capital, knowledge management practices and firm performance", *Journal of Intellectual Capital*, Vol. 18 No. 4, pp. 904-922.

Ilvonen, I. (2013), *Knowledge Security – A Conceptual Analysis*. PhD Dissertation. Tampere University, Finland.

Ilvonen, I., Thalmann, S., Manhart, M. and Sillaber, C. (2018), "Reconciling digital transformation and knowledge protection: a research agenda", *Knowledge Management Research & Practice*, Vol. 16 No. 2, pp. 235-244.

Inkinen, H. (2015), "Review of empirical research on intellectual capital and firm performance", *Journal of Intellectual Capital*, Vol. 16 No. 3, pp. 518-565.

Islam, M. and Stafford, T. (2017), "Information Technology (IT) integration and cybersecurity/security: the security savviness of board of directors", In *Proceedings, Accounting Information Systems* (*Sigasys*) *AMCIS2017, Boston, USA*.

ISO/IEC 27014. (2013), "ISO/IEC 27014:2013 (Information technology – Security techniques – Governance of Information Security)", available at: https://www.iso.org/standard/43754.html (Accessed 11 April 2019).

Jennex, M.E. and Zyngier, S. (2007), "Security as a contributor to knowledge management success", *Information Systems Frontiers*, Vol. 9 No. 5, pp. 493-504.

Johanson, U., Koga, C., Skoog, M. and Henningsson, J. (2006), "The Japanese Government's Intellectual Capital reporting guidelines – what are the challenges for firms and capital market actors?", *Journal of Intellectual Capital*, Vol. 7 No. 4, pp. 474-491.

Jordão, R.V.D. and Almeida, V.R.D. (2017), "Performance measurement, intellectual capital and financial sustainability", *Journal of Intellectual Capital*, Vol. 18 No. 3, pp. 643-666.

Kale, P., Singh, H., & Perlmutter, H. (2000), "Learning and protection of proprietary assets in strategic alliances: Building relational capital", *Strategic Management Journal*, Vol. 21 No. 3, pp. 217-237.

Kianto, A., Ritala, P., Vanhala, M. and Hussinki, H. (2018), "Reflections on the criteria for the sound measurement of intellectual capital: A knowledge-based perspective", *Critical Perspectives on Accounting*. https://doi.org/10.1016/j.cpa.2018.05.002, In Press.

Laney, D.B. (2018), *Infonomics: how to monetize, manage, and measure information as an asset for competitive advantage*. Abingdon, OXON.

Laperche, B. J. (2016), "Large Firms' Knowledge Capital and Innovation Networks" *Knowledge Economy*, 30 June, pp. 1-18. https://doi.org/10.1007/s13132-016-0391-7

Losee, R.M. (1997), "A discipline independent definition of information", *Journal of the American Society for Information Science*, Vol. 48 No. 3, pp. 254-269.

Lundgren, B. and Möller, N. (2019), "Defining Information Security," *Science and Engineering Ethics*, Vol. 25 No. 2, pp. 419-441.

Marr, B. and Schiuma, G. (2001), "Measuring and managing intellectual capital and knowledge assets in new economy organizations", in Bourne, M. (Eds). *Handbook of Performance Measurement*, Gee Publisher, London.

Martemucci, M.G. (2015), "Unpunished insults-the looming cyber Barbary wars", *Case Western Reserve Journal of International Law*, Vol. 47 No. 3, pp. 53-62.

Martin, N. and Rice, J. (2011), "Cybercrime: Understanding and addressing the concerns of stakeholders", *Computers & Security*, Vol. 30 No. 8, pp. 803-814.

Mayo, Andrew. (2000), "The role of employee development in the growth of intellectual capital", *Personnel Review*, Vol. 29 No. 4, pp. 521-533,

McLaughlin, Peter. (2016), “Cyber security and the board of directors”, available at: https://www.financierworldwide.com/cyber-security-and-the-board-of-directors#.XOAlUtO2nBI (Accessed 16 May 2019).

McMillan, L.L.P. (2019), “Financial Institutions: OSFI's Heightened Cyber Security Incident Reporting Obligations Now In Effect” available at: https://www.lexology.com/library/detail.aspx?g=d66640ad-3969-490d-a9fd-b3ad0aacc8cb (Accessed 12 April 2019).

Michaelsons. (2018), “POPI Regulations 2018 published in final form”, available at: https://www.michalsons.com/blog/popi-regulations-popia-regulations/12417 (Accessed 19 April 2019).

Mohamed, S., Mynors, D., Grantham, A., Walsh, K. and Chan, P. (2006), “Understanding one aspect of the knowledge leakage concept: people”, In *Proceedings of the European and Mediterranean Conference on Information Systems (EMCIS), Costa Blanca, Spain*, pp. 6-7.

M’Pherson, P.K. and Pike, S. (2001), “Accounting, empirical measurement and intellectual capital”, *Journal of Intellectual Capital*, Vol. 2 No. 3, pp. 246-260.

Nahapiet, J. and Ghoshal, S. (1998), “Social capital, intellectual capital, and the organizational advantage”, *Academy of Management Review*, Vol. 23 No. 2, pp. 242-266.

Nasheri, Hedi. (2012), “The Challenge of Economic Espionage”, *World Politics Review*, available at https://www.worldpoliticsreview.com/articles/12025/the-challenge-of-economic-espionage (Accessed 6 July 2019).

Ng, Daniel, and Tsui, Eric. (2010), “Knowledge-Intensive Collaboration to Combat Cyber Crime in the Asia Pacific Region”, In *ICICKM2010-Proceedings of the 7th International Conference on Intellectual Capital, Knowledge Management and Organisational Learning, Hong Hong,* pp. 323-330. Academic Conferences Limited.

NICE (2016), “National Initiative for Cybersecurity Education”, available at: http://csrc.nist.gov/nice/ (Accessed 3 September 2016).

Ordóñez de Pablos, P. (2003), “Measuring and reporting knowledge-based resources: the intellectual capital report”, The University of Oviedo, Spain, 1–13. Retrieved from https://warwick.ac.uk/fac/soc/wbs/conf/olkc/archive/oklc3/papers/id392.pdf (Accessed 16 May 2019).

Pedrini, Matteo. (2007),"Human capital convergences in intellectual capital and sustainability reports", *Journal of Intellectual Capital*, Vol. 8 No, 2, pp. 346–366.

Pike, S., Roos, G. and Marr, B. (2005), “Strategic management of intangible assets and value drivers in R&D organizations”, *R&D Management*, Vol. 35 No. 2, pp. 111-124.

Post, D. (2014), “Cybersecurity in the Boardroom: The New Reality for Directors”, available at: https://iapp.org/news/a/cybersecurity-in-the-boardroom-the-new-reality-for-directors/ (Accessed 16 May 2019).

Posthumus, S. and Von Solms, R. (2004), “A framework for the governance of information security”, *Computers & Security*, Vol. 23 No. 8, pp. 638-646.

Powell, Walter W and Snellman, Kaisa. (2004), “The Knowledge Economy”, *Annual Review of Sociology*. Vol. 30 No. 1: pp. 199–220.

Price, Nicholas. (2017), “Cybersecurity, Corporate Governance and Your Board of Directors”, available at: https://diligent.com/en-gb/blog/cybersecurity-corporate-governance-board-directors/ (Accessed 16 May 2019).

Rai, Sajay. (2014), “*Cybersecurity What The Board Of Directors Needs To Ask*”, ISACA The Institute of Internal Auditors Research Foundation (IIARF) Research Report. https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-What-the-Board-of-Directors-Needs-to-Ask.aspx (Accessed 7 July 2019).

Ramirez, R. and Choucri, N. (2016), “Improving interdisciplinary communication with standardized Cyber Security terminology: A literature review”, *IEEE Access*, Vol. 4, pp. 2216-2243.

Rastogi, P.N. (2002), “Knowledge management and intellectual capital as a paradigm of value creation”, *Human Systems Management*, Vol. 21 No. 4, pp. 229-240.

Reed, K.K., Lubatkin, M. and Srinivasan, N. (2006), “Proposing and testing an intellectual capital-based view of the firm”, *Journal of Management Studies*, Vol. 43 No. 4, pp. 867-893.

Roos, G. and Roos, J. (1997), “Measuring your company's intellectual performance”, *Long Range Planning*, Vol. 30 No. 3, pp. 413-426.

Schatz, D., Bashroush, R. and Wall, J. (2017), “Towards a more representative definition of cyber security”, *Journal of Digital Forensics, Security and Law*, Vol. *12 No*. 2, p. 53-74.

Scott, K., Dyas, J.V., Middlemass, J.B. and Siriwardena, A.N. (2007), "Confidentiality in the waiting room: an observational study in general practice", *Br J Gen Pract*, Vol. 57 No. 539, pp. 490-493.

Scholl, Frederick. (2017), "Cybersecurity: What does the board want?" available at: https://www.csoonline.com/article/3171700/cybersecurity-what-does-the-board-want.html (Accessed 18 May 2019).

Scully, T. (2014), "The cyber security threat stops in the boardroom", *Journal of Business Continuity & Emergency Planning*, Vol. 7 No. 2, pp. 138-148.

Secundo, G., Del Vecchio, P., Dumay, J. and Passiante, G. (2017), "Intellectual capital in the age of BD: establishing a research agenda", *Journal of Intellectual Capital*, Vol. 18 No. 2, pp. 242-261.

Shamala, P. and Ahmad, R. (2014), "A proposed taxonomy of assets for information security risk assessment (ISRA)", In *4th World Congress on Information and Communication Technologies (WICT 2014, Malacca, Malaysia),* pp. 29-33.

Shedden, P., Smith, W. and Ahmad, A. (2010), "Information security risk assessment: towards a business practice perspective", In *8th Australian Information Security Management Conference, Perth Australia,* pp. 119-130.

Sims, B. (2019) " 'UK Boards of Directors don't understand cyber threat' suggests Government's Cyber Governance Health Check", available at: https://www.risk-uk.com/uk-boards-of-directors-dont-understand-cyber-threat-suggests-governments-cyber-governance-health-check/ (Accessed 20 April 2019).

Solove, D. J. and Citron, D. K. (2017), "Risk and Anxiety: A Theory of Data-Breach Harms", *Texas Law Review*, Vol. 66, pp. 1231-1291.

Stark, John Reed and Fontaine, David R. (2015), "Ten Cybersecurity Concerns for Every Board of Directors", available at: http://www.cybersecuritydocket.com/2015/04/30/ten-cybersecurity-concerns-for-every-board-of-directors/ (Accessed 18 May 2019).

Stewart, T. and Ruckdeschel, C. (1998), "Intellectual capital: The new wealth of organizations", *Performance Improvement*, Vol. 37 No. 7, pp. 56-59.

Su, H.Y. (2014), "Business Ethics and the Development of Intellectual Capital", *Journal of Business Ethics*, Vol. 119 No. 1, pp. 87-98.

Sukhodolov, A.P., Popkova, E.G. and Kuzlaeva, I.M. (2018), "Perspectives of Internet economy creation", In *Internet Economy vs Classic Economy: Struggle of Contradictions* (pp. 23-41). Springer, Cham.

Trautman, L.J. and Altenbaumer-Price, K. (2010), "The board's responsibility for information technology governance", *John Marshall Journal of Computer & Information Law*, Vol. 28 No. 3, pp. 313-341.

Trautman, L.J., Triche, J. and Wetherbe, J. (2013), "Corporate information technology governance under fire", *Journal of Strategic and International Studies*, Vol. 8 No. 3, pp. 105-114.

Trautman, L. J. and Ormerod, P. C. (2016), "Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach", *American University Law Review*, Vol. 66, pp. 1231-1291.

Trautman, L.J. (2016), "Managing Cyberthreat", *Santa Clara Computer & High Tech. Law Journal*, Vol. *33*, No. 2, pp. 230-287.

Turner, N., Maylor, H. and Swart, J. (2015), "Ambidexterity in projects: An intellectual capital perspective", *International Journal of Project Management*, Vol. 33 No. 1, pp. 177-188.

Uretsky, M. (2002), "A framework for examining security issues and measures", *Journal of Organizational Excellence*, Vol. 21 No. 3, pp. 69-71.

Veltsos, C. (2015), "What Cybersecurity Questions Are Boards Asking CISOs?", available at: https://securityintelligence.com/what-cybersecurity-questions-are-boards-asking-cisos/ (Accessed 18 May 2019).

Von Solms, R. and von Solms, S.B. (2006), "Information security governance: Due care", *Computers & Security*, Vol. 25 No. 7, pp. 494-497.

Von Solms, B. and Von Solms, R. (2018), "Cybersecurity and information security – what goes where?", *Information and Computer Security*, Vol. 26 No. 1, pp. 2-9.

Weill, P. and Ross, J.W. (2004), *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business Press, Boston, Massachusetts.

Wiig, K.M. (1997), "Integrating intellectual capital and knowledge management". *Long Range Planning*, Vol. 30 No. 3, pp. 399-405.

Wootliff, B. (2019), “Is A Lack Of Cyber Due Diligence Putting Your Deal At Risk?”, available at: https://www.forbes.com/sites/riskmap/2019/03/21/is-a-lack-of-cyber-due-diligence-putting-your-deal-at-risk/#51f2fd326007 (Accessed 12 April 2019).

Zukis, B. (2019), “Regulators Want CEOs To Go To Jail For Cyber Failings, Should You?” available at: https://www.forbes.com/sites/bobzukis/2019/04/10/regulators-want-ceos-to-go-to-jail-for-cyber-failings-should-you/#39e5b49119fa (Accessed 12 April 2019).