What do we know about information security governance?

"From the basement to the boardroom": towards digital security governance

Stef Schinagl and Abbas Shahim
School of Business and Economics, Vrije Universiteit Amsterdam, Amsterdam, The Netherlands

Received 25 February 2019
Revised 16 June 2019
26 August 2019
18 October 2019
Accepted 20 October 2019

Abstract

Purpose – This paper aims to review the information security governance (ISG) literature and emphasises the tensions that exist at the intersection of the rapidly changing business climate and the current body of knowledge on ISG.

Design/methodology/approach – The intention of the authors was to conduct a systematic literature review. However, owing to limited empirical papers in ISG research, this paper is more conceptually organised.

Findings – This paper shows that security has shifted from a narrow-focused isolated issue towards a strategic business issue with "from the basement to the boardroom" implications. The key takeaway is that protecting the organisation is important, but organizations must also develop strategies to ensure resilient businesses to take advantage of the opportunities that digitalization can bring.

Research limitations/implications – The concept of DSG is a new research territory that addresses the limitations and gaps of traditional ISG approaches in a digital context. To this extent, organisational theories are suggested to help build knowledge that offers a deeper understanding than that provided by the too often used practical approaches in ISG research.

Practical implications – This paper supports practitioners and decision makers by providing a deeper understanding of how organisations and their security approaches are actually affected by digitalisation.

Social implications – This paper helps individuals to understand that they have increasing rights with regard to privacy and security and a say in what parties they assign business to.

Originality/value – This paper makes a novel contribution to ISG research. To the authors' knowledge, this is the first attempt to review and structure the ISG literature.

Keywords Technology, Information security governance, Literature review, Digitalisation, Cyber, Digital security governance

Paper type Literature review

1. Introduction

The information security (from now on referred to as IS or just security) landscape has shifted "from the basement to the boardroom", that is, from a narrowly focused technical issue towards a strategic business issue and a top priority item for the board

Information & Computer Security
Vol. 28 No. 2, 2020
pp. 261-292
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-02-2019-0033

(McFadzean *et al.*, 2007; Johnston and Hale, 2009; Kayworth and Whitten, 2012; Knapp *et al.*, 2009; Soomro *et al.*, 2016). The strategic approach towards the IS phenomenon is commonly referred to as information security governance (ISG) (Nicho, 2018). Today's organisations face increasingly dynamic environments and have to deal with a new and disruptive world that gladly embraces technology. This literature review reveals that in the context of the current ISG approaches, the technological impact dictates a need for change, mainly in the following ways (see also Table I).

First, organisations are rapidly adopting digital business strategies with a high level of technological deployment, e.g. the corporate utilisation of the cloud, blockchain, artificial intelligence, the internet of things (IoT), big data, mobile and social media technology (Carcary *et al.*, 2016; Karanja, 2017). This way of working leads to a full embedding of IT into a company's businesses (Soomro *et al.*, 2016; Wu and Saunders, 2016). Consider examples such as Airbnb, the "hotel broker"; Uber, a company that offers taxi services; and Alibaba, the e-commerce conglomerate. These current technology-driven business climates no longer leave room for distance between the traditional physical world and the new digital world (Soomro *et al.*, 2016; Shahim, 2017). A long existing gap between IT and business and therefore between security and business has been eliminated. This technological change has transformed the face of security from being an isolated issue to a strategic business challenge and requires security to be governed accordingly (Von Solms, 2001b; Wu and Saunders, 2016).

Second, because of the total embedding of technology in business, IS incidents and breaches now directly impact the business and can seriously affect the organisation (Soomro *et al.*, 2016; Horne *et al.*, 2017; Kauspadiene *et al.*, 2017; Stewart and Jürjens, 2017; Berkman *et al.*, 2018). Successful cyberattacks may lead to client, partner, financial and reputational loss as well as litigation and government sanctions; these attacks therefore limit the firm's

Need for change		Key challenges	References
Digital business	→	Embedding security in business	Soomro *et al.* (2016)
		No gap between the physical and digital world	Soomro *et al.* (2016), Shahim (2017)
		Security is a strategic collaborative business issue	Von Solms (2001b), Wu and Saunders (2016)
Increased impact of cyberattacks	→	Attracting management commitment	Veiga and Eloff (2007), Mukundan and Sai (2014), Barton *et al.* (2016), Damenu and Beaumont (2017)
		Increased direct business impact of cyber security attacks demand alternative ways to govern security	Goel and Shawky (2009), Zafar and Clark (2009), Georg (2017), Higgs *et al.* (2016), Soomro *et al.* (2016), Horne *et al.* (2017) Kauspadiene *et al.* (2017), Stewart and Jürjens (2017), Berkman *et al.* (2018), Hasbini *et al.* (2018)
		Cyber security attacks limit firms' competitive advantage, e.g. their innovation capability and productivity	Goel and Shawky (2009), Higgs *et al.* (2016), Horne *et al.* (2017) Kauspadiene *et al.* (2017), Hasbini *et al.* (2018)
Social change	→	Move from an intra- to an inter-organisational perspective	Karlsson *et al.* (2016)
		Trust leap: increase the reasonable expectation of security and privacy	Matwyshyn (2009), Botsman (2017), Romansky (2017)
		Digital supply chain. No individual businesses. Security risks cross boundaries	Karlsson *et al.* (2016), Büyüközkan and Göçer (2018)

Table I.
Key challenges for the need for change

productivity, innovation capability and competitive edge (Goel and Shawky, 2009; Higgs *et al.*, 2016; Kauspadiene *et al.*, 2017; Hasbini *et al.*, 2018). For example, IS breaches can cause negative market reactions and can materially affect a firm's financial position (Higgs *et al.*, 2016; Berkman *et al.*, 2018). Furthermore, scholars have found correlations between IS incidents and companies' performance (Georg, 2017). The announcement of an IS breach has a significant negative impact on market value, varying from 1 to 2.1 per cent (Goel and Shawky, 2009; Zafar and Clark, 2009). The increasing impact and costs of security attacks have forced corporate boards to think about alternative ways to govern security and stop the ever-increasing number of attacks. The commitment of senior executives and boards in this case is critical for effective ISG (Veiga and Eloff, 2007; Mukundan and Sai, 2014; Barton *et al.*, 2016; Damenu and Beaumont, 2017).

Third, digitalisation demands that organisations adopt an inter-organisational perspective towards security. On the one hand, this is driven by social change. Different scandals such as "Dieselgate", revelations such as those in the "Panama Papers", fake news statements posted on social media platforms and certainly large data breaches have caused a so-called "trust leap" in the modern society (Botsman, 2017). Ongoing IS breaches increase customers' reasonable expectations that corporations will take steps to protect their security and privacy (Gillon *et al.*, 2011). Upcoming laws and regulations, such as the *General Data Protection Regulation*, that aim to strengthen the rights of individuals stimulate these expectations even further (Romansky, 2017; Kemp, 2018). On the other hand, in a digital environment, organisations operate as a digital supply chain instead of as individual businesses (Büyüközkan and Göçer, 2018). Now, as security risks exist across boundaries, organisations have also become dependent on their partners' expertise to create security and expect these partners to be transparent about doing so (Matwyshyn, 2009; Karlsson *et al.*, 2016). On the whole, effective ISG must incorporate transparent inter-organisational protection to retain the trust of customers and partners.

The technology-driven shift has revealed a need for a revamped approach that looks beyond the newest "best practice" and that provides a deeper understanding of the ISG phenomenon in the new digital business context (Holgate *et al.*, 2012; Williams *et al.*, 2013; Tan *et al.*, 2017). However, the ISG literature lacks such an approach. ISG approaches mainly focus on security controls and common practices that are either generic or universal in scope and that are static (Siponen and Willison, 2009; Williams *et al.*, 2013; Flores *et al.*, 2014; Mishra, 2015). The emphasis on controls works well in a reasonably static technical environment but is insufficient in a rapid, agile and ever-changing digital environment (Holgate *et al.*, 2012; Tan *et al.*, 2017; Nicho, 2018).

Although a significant amount of research exists on security at different levels, studies regarding governing security are relatively thin (Nicho, 2018). In recent years, ISG studies have grown rapidly, leading to a growing diversity in ISG perspectives and changing contextual boundaries. However, these studies thus far have been neither structured nor synthesised. On the contrary, ISG has been poorly defined and discussed and means different things to different people (Moulton and Coles, 2003; Williams *et al.*, 2013). Furthermore, the ISG literature is relatively immature, i.e. largely descriptive, expressed in normative standards and common frameworks, and provides limited empirical or theoretical guidance (Mishra, 2015; Williams *et al.*, 2013). Therefore, analysing ISG literature by challenging the underlying assumptions and examining the tensions that exist at the intersection of the changing contextual boundaries and the current body of knowledge on ISG could be a powerful way to review prior ISG research and develop it further.

This paper makes a novel contribution to ISG research. To our knowledge, this is the first attempt to review and structure the ISG literature. The paper provides direction for a new

stream of research that addresses the need for change in the current ISG approaches towards digital security governance (DSG). In addition, the paper contributes to a recurring call for more theory building in ISG research (Williams *et al.*, 2013) and urges scholars to draw on theories from related fields. We suggest a focus on the following organisational theories: *high reliability, normal accidents, two-factor motivation and issue selling*. These theories help provide a more in-depth understanding of the organisational factors that are critical for detecting and preventing security accidents (Leveson *et al.*, 2009).

The paper continues with the following sections. Section 2 describes the methodology followed for the literature review, which precedes an exploratory Section 3 on ISG definitions, perspectives and models. In the Section 4, we discuss the main tensions that hinder the field's advancement towards business-oriented ISG. Section 5 contains a discussion and suggestions for further research. The paper ends with implications for research in Section 6 and conclusion in Section 7.

2. Methodology

The intention of the authors was to conduct a systematic literature review of the ISG literature. However, given limited empirical papers in ISG research, this paper is more conceptually organised. The methodology used in this paper is as follows.

2.1 Searching the literature

The following steps were taken to conduct the literature review.

- *Inclusion criteria*: The Web of Science database was used to search for potential papers. In this case, the authors searched with the term "information security governance". We checked whether other search terms, such as "cyber-", "business-" and "digital security governance", generated new papers, but this was not the case. The search was not restricted by the articles' age or the grade of the journal; instead, we preferred to examine each paper found for nuances that could shed light on our evolving understanding of the concept (Horne *et al.*, 2017). This led to an initial set of 126 papers up until 2018.
- *Exclusion criteria*: By reading abstracts, papers were excluded from this review for multiple reasons. However, the main reasons for a paper's exclusion were either the paper's language, e.g., *Spanish or Russian, or the relevancy of the paper's topic.* Relevant studies in the context of security governance were found in areas such as *internet governance, data governance and e-governance.* However, these papers were excluded. The intention of this paper was to focus more in-depth on how digitalisation impacts security at the organisational level. Including these topics would not have benefited the precision of the analyses with regard to this scope.
- *"Snowball effect"*: By reading the introductions of the papers, we added relevant references. These were mainly in the context of "information security strategy" and "information security investment". In all, 17 relevant papers were added.
- *Search results*: A total of 76 papers were included in the final sample. By using predefined criteria, these papers were fully read, analysed and structured to provide the insights in this paper.

2.2 Analysing the identified literature

The first analysis of the literature led to four areas that aroused the interest of the authors. First, the papers on ISG have rapidly grown, especially in the past three years (Table II).

Table II.
ISG publication and distribution (1996-2018)

ISG papers published in journals over the years	1996	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	Total
AIS Electronic Library																		1		1
Australasian Journal of Information Systems																		1		1
Australian Information Security Management Conference									1											1
Baltic Journal of Modern Computing																		1		1
BLED 2012 Proceedings													1							1
California Management Review			1																	1
Communications of the ACM										1										1
Communications of the Association for Information Systems										1		1								2
Computer Law & Security Review																			1	1
Computer Science & Information Systems																1				1
Computers & Security	1	2		1	2	3	3	1		1					1	1	1	1		18
Computers in Industry																			1	1
Decision Support Systems																	1			1
Electronic Markets														1						1
European Journal of Information Systems																		1		1
Health and Technology																		1		1
IEEE Transaction on Engineering Management														1						1
Information & Computer Security																1	2	4	2	9
Information & Management										2								1		3
Information & Software Technology																1				1
									1											1

(*continued*)

Table II.

ISG papers published in journals over the years	1996	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	Total
Information Management & Computer Security																				
Information Resources Management Journal																			1	1
Information Systems Frontiers																		1		1
Information Systems Management								1												1
Information Technology and Management															1					1
International Conference on Knowledge-Based and Intelligent . . . systems								1												1
International Journal of Enterprise Information Systems																			1	1
International Journal of Information Management											1						1		1	3
International Journal of Information Systems & Project Management																	1			1
International Journal on Information Technologies & Security																		1		1
IT Professional																	1			1
Journal of Accounting and Public Policy																			1	1
Journal of Business Ethics											1									1
Journal of Information Assurance & Security																		1		1
Journal of Information Systems																	1			1
Journal of Intelligent Manufacturing															1					1

(*continued*)

ISG papers published in journals over the years	1996	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	Total
Journal of Management & Governance																	1			1
Journal of Universal Computer Science													1							1
MIS Quarterly Executive											1									1
MIT Sloan Management Review								1											1	1
Online Information Review																				1
Pacific Asia Journal of the Association for Information Systems																			1	1
Procedia Computer Science																			1	1
Royal Society Publishing																			1	1
The Computer Journal																1				1
World Journal of Entrepreneurship, Management and Sustain Dev.																			1	1
Total	1	2	1	1	2	3	4	3	2	5	3	1	2	2	3	5	9	14	13	76

Table II.

Second, there are a variety of different journals represented on the list (Table II). The papers were collected from 46 different journals. The Computers and Security journal (18) and the Information and Computer Security (9) journal published the most papers on ISG. All of the other journals mostly delivered one or two papers. Third, ISG papers have low "research maturity". Following Karlsson *et al.* (2016), the research papers are classified by maturity; from emergent to mature (Figure 1).

Figure 2 shows that over time, the ISG literature has become more mature. However, according to the above classification, only 41 per cent of the papers contain empirical data (theory generating and theory testing). Fourth, the authors are not aware and did not find any literature review that focused on ISG. These remarks indicate changing contextual boundaries and growing variety of ISG perspectives and interpretations that need to be structured. This showed the way and further motivated the authors to conduct the ISG literature review presented in this paper.

3. Definitions, perspectives and models

The lens provided in the introduction of this paper (Table I) demonstrates the change in the ISG contextual boundaries towards embedded business and inter-organisational ISG approaches. In this explorative section, the aim is to structure the current body of knowledge on the ISG concept and to examine its underlying definitions, perspectives and models.

State of research	Research purpose	Operational definition
Emergent ↑	Descriptive	Describes a phenomenon in its appearance without the use of theory
	Philosophical	Reflects upon a phenomenon without data or reference to any theory
	Theoretical	Reflects upon a phenomenon based on some theory but without empirical data (or with anecdotal data)
	Theory generating	Attempts to analyse/interpret quantitative or qualitative data in a systematic manner for model building
↓ Mature	Theory testing	Attempts to test a theory by using quantitative or qualitative data in a systematic manner, i.e., not only strict theory testing

Figure 1.
Research maturity

Source: Karlsson *et al.* (2016)

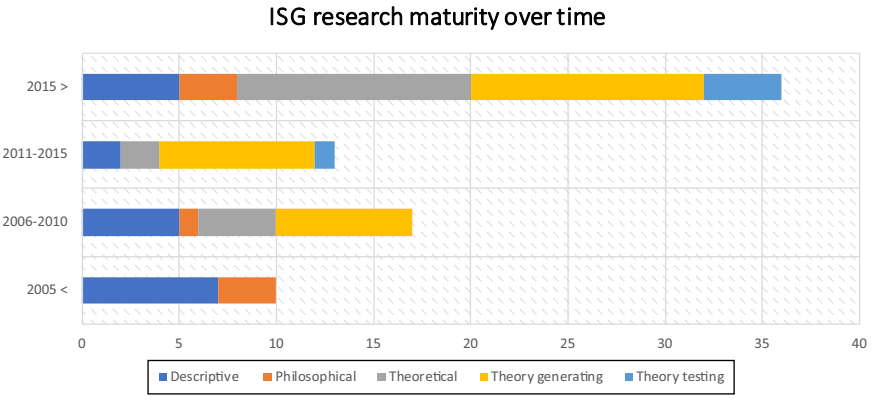

Figure 2.
ISG research maturity classified over time

Source: Based on 76 papers ISG-literature review

3.1 Information security governance definitions

Various interpretations of the term ISG exist in the literature (Holgate *et al.*, 2012; Williams *et al.*, 2013). In contrast to Moulton and Coles (2003), the literature shows that the content of ISG definitions has been relatively steady over time, i.e. the definitions of ISG have always been related to the thought that senior executives and boards are responsible for security and the way it is incorporated into organisational structures (Posthumus and Von Solms, 2004; Von Solms and Von Solms, 2006a; McFadzean *et al.*, 2007). Second, ISG definitions start with general descriptions of the ISG concept, leaving room for interpretation and discussion: *"ISG means making sufficient rigor to safeguard your organisation"* (Moulton and Coles, 2003; Park *et al.*, 2006) or "the term ISG describes the process of how security is addressed at an executive level" (Posthumus and Von Solms, 2004). However, over time, the definitions have become specific about the detailed elements that are a part of ISG, e.g.:

> [. . .] corporate security governance focuses on setting the responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly (Tan *et al.*, 2017).

Additionally, the understanding of ISG has changed over time. Initially, definitions mainly focused narrowly on IT: "*ISG can be seen as the overall way in which Information Security as a discipline is deployed to mitigate IT risks*" (Von Solms, 2006; Veiga and Eloff, 2007). Later, definitions expanded towards enterprise-wide or "business" risk, including terms such as "strategic direction" and "adjusting organisational structures" (Tan *et al.*, 2017; Maynard *et al.*, 2018; Nicho, 2018). Williams *et al.* (2013) argue that the meaning of ISG is fluid, dynamic and flexible because of the ongoing changing socio-technical environment. This change has not yet been clarified in the ISG literature. This paper moves away from strictly defining ISG and instead provides an overview of the different perspectives in the field.

3.2 Information security governance perspectives

IS research has seen a steady progression, moving from a narrow focus on "technical controls" towards a more holistic approach, including organisational and behavioural or social elements (Veiga and Eloff, 2007; Flores *et al.*, 2014; Soomro *et al.*, 2016). Mainly at the individual level, IS research is supported by a wide range of topics and theories: *deterrence, neutralisation, rational choice, reasoned action, planned behaviour and protection motivation* (Cram *et al.*, 2017). This field has mainly focused on why end users engage in risky behaviour such as employee non-compliance. (Flores *et al.*, 2014; Barton *et al.*, 2016; Chulkov, 2017). While knowledge about the individual level of security is increasingly being built, less is known about the "governance" level. The following governance perspectives are derived from the extant ISG literature.

3.2.1 The corporate governance perspective. Most scholars directly relate security to corporate governance, with a predominant view of ISG as a subset of IT governance (Von Solms, 2001b; Posthumus and Von Solms, 2004; Moulton and Coles, 2003; Von Solms, 2005; Von Solms and Von Solms, 2006a; Von Solms and Von Solms, 2006b). This early stream of scholars mainly frame ISG as being driven by compulsory forces within corporate governance and emphasise its (technical) controls. The first and perhaps most given reason for this perspective is that directors are responsible, often legally, for their organisation's risk management system and internal controls (McFadzean *et al.*, 2007), such as the reporting on internal controls and compliance demanded by the Sarbanes–Oxley Act. In enterprise-wide risk management, ISG plays a pivotal role in ensuring that controls are implemented and that potential losses that could arise from these risks are managed.

Arising out of a company's moral duty to avoid knowingly causing harm to others, a second argument is that companies have ethical obligations to improve ISG (Matwyshyn, 2009). The expectations of ethical behaviour are at the core of most corporate governance theories (Bihari, 2008).

From this perspective, it has long been believed that as part of the company's corporate governance, ISG is the most suitable path by which to gain control of security processes and guarantee their alignment with business strategies (Rebollo *et al.*, 2015b). However, the main concern of this perspective is that security is often relegated as a subset of IT governance, and limited attention is given to how the business context may affect the need for security (Williams *et al.*, 2013). This approach emphasises technical controls that alone are not sufficient to achieve effective ISG in a socio-technical environment. Therefore, considering this line of reasoning, in rapidly changing environments, the traditional view of governance as a control and conformance mechanism turns out to be inadequate.

3.2.2 The socio-technical perspective. A second dominant perspective is that instead of focusing mainly on (technical) security controls, ISG should be governed from a holistic perspective and should accent the socio-technical elements, e.g. the organisational and human elements (Veiga and Eloff, 2007; Flores *et al.*, 2014; Soomro *et al.*, 2016). ISG approaches that ignore the human and individual levels often have little bearing on the organisations' objectives (Mishra, 2015). To this extent, researchers highlight the importance of achieving a supportive security culture, combining corporate governance and information security, as this approach takes into account the complex socio-technical system (Thomson and Von Solms, 2005; Veiga and Eloff, 2007; Ruighaver *et al.*, 2007; Flores *et al.*, 2014; Damenu and Beaumont, 2017).

The socio-technical perspective strives for a more holistic approach, encompassing explicit attention to the human element. However, owing to its increased focus on the individual level, this perspective of ISG often also has a bias. This creates a narrow view that does not provide insight into how ISG is related at the organisational level (Ruighaver *et al.*, 2007). For instance, organisations that have lower requirements for security often are tolerant of change, while those organisations that have a high requirement for security have a tendency to favour stability over change (Ruighaver *et al.*, 2007). In a rapidly changing digital environment, these organisational relationships are relevant for incorporating into ISG approaches and are often forgotten in the socio-technical perspective.

3.2.3 The resilient business perspective. A more recent consideration is that there is neither a predominant view that ISG is related to IT governance nor that the relationship of ISG with corporate governance is of decisive importance (Williams *et al.*, 2013). It is more important to understand how ISG is related to business processes, e.g. how to align security with strategic drivers, such as the organisation's mission, goals and objectives, to enable organisational resilience (Williams *et al.*, 2013).

The ISG literature is increasingly acknowledging the importance of a business-oriented approach, but this literature is still in a descriptive phase. Von Solms and Von Solms (2005) propose the term business security governance to better frame the integral part of wide business protection. Furthermore, instead of a preventive approach that is based on risk and controls, organisations should address IS objectives and strategies by developing a resilient business framework (Tan *et al.*, 2017; Maynard *et al.*, 2018). Security throughout the enterprise may be the key to improving the level of security in organisations (Maynard *et al.*, 2018).

3.3 Information security governance models

There are a variety of practitioners, research frameworks, models and normative standards that have assisted organisations with ISG. In this section, the models are examined in line with the perspectives in the previous section. The following overview is used to reflect on the different models and discuss their shortcomings.

3.3.1 Information security governance models in practice. Well-known ISG practical frameworks include ISO standards such as the 27001 and 38500 series, multiple standards from the National Institute of Standards and Technology (NIST), the Control Objectives for Information and related Technology methodology for IT controls and Information Technology Infrastructure Library practices for managing IT operations (Haufe *et al.*, 2016; Bobbert, 2018). Many of these good practices are well established and are supported by a wide range of industry solutions. However, first, the well-known standards are generic in scope, while organisations need methods tailored to their environment and operations. Second, most ISG models have not been validated but are fostered by an appeal to common practice, which is an unsound basis for a true standard (Siponen and Willison, 2009). Third, the proposed standards and best practices are designed to guide organisations in their ISG strategy but do not define the practical framework to implement or measure the organisation's ISG strategy (Maleh *et al.*, 2017). Therefore, the current practical frameworks not only lack theoretically grounded methods but also lack empirical evidence on their effectiveness (Flores *et al.*, 2014).

3.3.2 Information security governance models in research. In this section, the existing ISG research models are further analysed. Thereafter, the model flaws are discussed.

Corporate governance-oriented models: Scholars have developed a variety of ISG models and frameworks that have mainly provided an objective, conceptual framework and building blocks for ISG. In their framework, Posthumus and Von Solms (2004) and Von Solms and Von Solms (2006a) assert that there is a need to integrate security into corporate governance. Park *et al.* (2006) provide a framework to structure ISG for corporate executives, thereby enabling the creation of greater productivity gains and cost efficiencies for security. Conceptual models of this nature are anecdotal, too broad in scope and lack supporting theory or empirical evidence (Mishra, 2015).

Socio-technically oriented (holistic): Because technical measures alone are not sufficient, several approaches focusing on the "human" side of holistic ISG have been proposed by researchers (Flores *et al.*, 2014). Dutta and McCrohan (2002) propose an organisational security approach that recognises three cornerstones, namely, critical infrastructures, organisation, and technology, to help senior management address security as the socio-technical problem that it truly is. Veiga and Eloff (2007) propose a detailed framework towards a holistic and people-orientated approach. Maleh *et al.* (2017) suggest that it is essential to put in place an ISG approach adapted to the culture of the organisation. Their proposed capability maturity framework (CAFISGO) helps organisations assess their capability maturity state and address the procedural, technical and human aspects of ISG. The drawback of these frameworks mainly lies in the lack of emphasis placed on the integration of feedback and modification with changing business requirements (Mishra, 2015).

Process-oriented: To avoid the criticism that ISG has been viewed as a static process, some researchers have approached ISG as an ongoing process. Knapp *et al.* (2009) focus on the IS policy process by showing a larger organisational context that includes key external and internal influences that can materially impact organisational processes. Haufe *et al.* (2016) suggest a process framework to help focus on the operation of an Information Security Management System instead of focusing only on measures and controls. Carcary *et al.* (2016) explain that approaches to ISG must be fluid and responsive to the changing IS

landscape. The authors present a practitioner-oriented capability maturity framework that helps organisations focus on continually evaluating, re-evaluating, and developing the ISGM capability in line with environmental changes and new opportunities and threats. Nicho (2018) construct and empirically validate an ISG process model using Deming's plan–do–check–act (PDCA) cycle model, which was continuously updated to align it with the highly dynamic nature of security. By using this model, the authors address the extant literature's gap due to the lack of studies on a methodological approach to implementing ISG in an organisation.

Cyber-oriented: Other studies are concerned with the increasing threats created by the digital landscape and therefore suggest improvements to existing ISG models or the development of topic-specific ISG models. For example, Kauspadiene *et al.* (2017) suggest that today's digital world requires a resilient view of security and must consider multiple partners, collaborative systems, outsourcing and other third parties. To increase the security level, the authors propose an integrated holistic methodology for construction of a high-level, self-sustaining information security management framework. Rebollo *et al.* (2015a) present a framework focused on the ISG of the cloud-computing environment, as security risks hinder the development of cloud-computing services, and a comprehensive security governance process is needed to foster the adoption of cloud services. Moghadam and Colomo-Palacios (2018) provide an overview of ISG in big data environments. The authors conclude that ISG necessitates constant control associated with using governance techniques such as risk management, business process management and security process management to ensure business value.

3.3.3 Information security governance model flaws. The ISG literature provides multiple models. However, there is no common and general view on what and how it should be done to ensure unimpeded and resilient processes of security (Kauspadiene *et al.*, 2017). Although researchers have answered the long-heard call for more empirical and validated models (Knapp *et al.*, 2009; Maleh *et al.*, 2017; Haufe *et al.*, 2016; Nicho, 2018), most of the ISG models created up until now still lack theory and empirical validation, are generic or universal in scope, are static and do not acknowledge the importance of social and behavioural factors (McFadzean *et al.*, 2007; Siponen and Willison, 2009; Williams *et al.*, 2013; Flores *et al.*, 2014; Mishra, 2015). This leads to two main general issues that hinder ISG in the digital business context. First, the contextual security governance challenges that an organisation faces are not considered. This point of organisational fit is critical, and ISG is not one size fits all. The challenges of ISG may be universal in terms of protecting information assets, but the way each organisation responds varies according to its specific business context, requirements and risk-tolerance levels (Holgate *et al.*, 2012; Soomro *et al.*, 2016; Damenu and Beaumont, 2017). Put simply, isolated organisation-wide security frameworks are inadequate today (Kauspadiene *et al.*, 2017). Second, organisations that continue to use the same old isolated security approach overlook new challenges that exist in their security environment and that warrant new and unconventional approaches (Ruighaver *et al.*, 2007). A paradigm shift is required to move from internally focused protection of organisation-wide information towards an embedded and resilient view that considers an organisation's collaborative business environment (Horne *et al.*, 2017; Kauspadiene *et al.*, 2017). Clear theoretical guidance on such an approach is currently lacking in the literature. For a summary of the common body of knowledge described in this chapter, see Table III.

4. Tensions "from the basement to the boardroom" in a digital era

The analyses in the previous sections show the changing landscape of ISG. However, both ISG research and practice have adopted only a limited approach to address the challenges of

Table III.
Perspectives and models in ISG research

Perspectives	Corporate governance		Socio-technical	Resilient business	
Essentials	ISG as a subset of IT governance Emphasis on (technical) controls		Human element Security culture	Embedding security in businesses Developing depth in a business context	
Drivers	Legal responsibility Ethical obligations		Holistic approach Complex socio-technical system	Resilience Impact of business on security	
Remarks	Limited attention to how the business context may affect security Technical-driven controls alone are not sufficient in a rapidly changing or socio-technical environment		Bias due to excessive focus on the individual level Lack of insight into the relation of ISG to the organisational level	Still in a descriptive phase Relation between security, IT and corporate governance not of decisive importance	
References	Von Solms (2001b), Moulton and Coles (2003), Posthumus and Von Solms (2004), Von Solms (2005), Von Solms and Von Solms (2006a), Von Solms and Von Solms (2006b), McFadzean *et al.* (2007), Bihari (2008), Matwyshyn (2009) Williams *et al.* (2013), Rebollo *et al.* (2015b)		Thomson and Von Solms (2005), Veiga and Eloff (2007), Flores *et al.* (2014) Soomro *et al.* (2016), Veiga and Eloff (2007), Ruighaver *et al.* (2007), Flores *et al.* (2014), Damenu and Beaumont (2017)	Von Solms and Von Solms (2005), Tan *et al.* (2017), Bobbert (2018), Maynard *et al.* (2018)	
Models	*Practice-oriented*	*Governance-oriented*	*Socio-technically oriented*	*Process-oriented*	*Cyber-oriented*

(*continued*)

Table III.

Perspectives	Corporate governance		Socio-technical	Resilient business	
Characteristics	Common practice, wide range of support in industry ISO 27001, NIST, COBIT and ITIL	High-level building blocks Integrate security into corporate and IT governance	Socio-technical focus Acknowledge the importance of culture	Continuous evaluation and updating PDCA-Deming circle (ongoing process) Internal and external factors	Inter-organisational approach; Considers multiple partners PDCA-Deming circle (Continuous process)
Drivers	Enhance performance by governance processes Guide organisations in ISG strategy	Address security at an executive level	Holistic approach in addition to technical controls	Be fluid and responsive due to changing landscape Increase level of security	Increasing cyber threats Defence strategy for a resilient process Alignment with a highly dynamic nature of security
Remarks	Generic in scope; not tailored to the environment Lack of validation and implementation guidance Lack of social and behavioural factors	Too broad in scope Lack of supporting theory or empirical evidence Descriptive and conceptual research	Lack of integration of feedback and modification with changing business requirements	Achieve real-world representation of an IS policy process Avoid criticism of being static Empirically validated model	Constant necessity to ensure business value
References	Siponen and Willison (2009), Flores *et al.* (2014), Maleh *et al.* (2017)	Posthumus and Von Solms (2004), Park *et al.* (2006), Von Solms and Von Solms (2006a)	Dutta and McCrohan (2002), Veiga and Eloff (2007), Maleh *et al.* (2017)	Knapp *et al.* (2009) Carcary *et al.* (2016), Haufe *et al.* (2016), Nicho (2018)	Kauspadiene *et al.* (2017), Rebollo *et al.* (2015a), Moghadam and Colomo-Palacios (2018)

the digital era. This can be considered a "gap" that occurs between the intersection of the current common body of knowledge in ISG (state A) and the changing contextual boundaries towards a state B: DSG. Based on the literature review, an important insight is that ISG or is not the same as DSG. The latter is about achieving resilience by embedding security in the business and in all of the related business dimensions and organisational factors as a whole (machines, people, objects, processes, etc.). Frequently used terms such as integration and IT alignment become superfluous in such environments. To gain a deeper understanding of the gap between ISG and DSG, the authors observed the tensions that were revealed in the extant literature and that originate from the following three key challenges that are described in the introduction (Table I). Discussing the tensions facilitates cumulative knowledge building and contributes to further developing ISG research. The tensions are as follows (Table IV).

4.1 Digital business

The IS discipline in research and business has undergone an impressive development in recent decades (Georg, 2017; Moghadam and Colomo-Palacios, 2018). Historically, companies have followed a technically focused approach that emphasises the primary role of technology in designing effective security solutions (Lindup, 1996; Dutta and McCrohan, 2002; Ozkan and Karabacak, 2010; Kayworth and Whitten, 2012). The impact of technology on ISG described in this paper demands an embedded security and a resilient business approach that is at the core of the fabric of the organisation, while not hindering the business from conducting its activities (Ahmad *et al.*, 2014; Kayworth and Whitten, 2012; Flores *et al.*, 2014). However, security is still often seen by many organisations as a remote activity of a technical nature (Alavi *et al.*, 2016). This view leads to the following tensions.

4.1.1 Preventive versus a continuous and resilient approach. IS strategic development is significantly lacking in many organisations (McFadzean *et al.*, 2007; Barton *et al.*, 2016). Ruighaver *et al.* (2007) found that security is *ad hoc* and focuses on things demanding immediate attention owing to incidents at the perimeter of the organisation (Johnston and Hale, 2009). Security is often only regarded as a strategic business issue if something goes wrong (Tan *et al.*, 2017; Maynard *et al.*, 2018). Often, such environments persist because organisations are used to focusing on preventing outside attacks (Rothrock *et al.*, 2018). However, attacks are immutable features of the digital business environment, and some fraction of these attacks will inevitably result in breaches (Rothrock *et al.*, 2018). For organisations, security in a digital environment means that the old challenge of detecting and neutralising threats to keep hackers out of their networks has expanded to include learning how to continue doing business during a breach and how to recover after one. In other words, the challenge has expanded from security alone to security and resilience (Rothrock *et al.*, 2018).

4.1.2 From an isolated towards a collaborative security function. IS scholars have found that security continues to be driven from the bottom up rather than from the top down (Ahmad *et al.*, 2014; Barton *et al.*, 2016). Empirical studies show that the security function is often relegated to lower IT levels (Williams *et al.*, 2013), as the highest ranking security role in the organisation often exists at a middle management level or lower (Ahmad *et al.*, 2014). Devolving security to lower levels maintains the perception of security as a technical function operating independently from the business (McFadzean *et al.*, 2007). The lack of integration between IS professionals and the operations of a business results in security policies and budgets not reflecting the needs of the business (Kayworth and Whitten, 2012).

From a DSG perspective, security should not be left to the IS professionals alone. In developing their ISG strategy, organisations should adopt an embedded and collaborative

Table IV.
Tensions in ISG literature

Tensions	State A: ISG		State B: DSG	References
Digital business	**Preventive approach** *Ad hoc* Only act when something goes wrong Prevent outside attacks	↔	**Continuous and resilient approach** Attacks are immutable features Continue business during a breach and recover	McFadzean *et al.* (2007), Ruighaver *et al.* (2007), Johnston and Hale (2009), Barton *et al.* (2016), Tan *et al.* (2017), Maynard *et al.* (2018), Rothrock *et al.* (2018)
	Isolated security function Bottom up Devolve security to low levels Not reflective of business needs	↔	**Collaborative security function** Top down Includes overall business management In line with business strategies Improves security assimilation	McFadzean *et al.* (2007), Kayworth and Whitten (2012), Williams *et al.* (2013), Ahmad *et al.* (2014), Barton *et al.* (2016), Soomro *et al.* (2016), Horne *et al.* (2017)
	Non-functional security Focus on ease of use and building cheaply and quickly Short-term focus	↔	**Embedded/by design** Security is not added after deployment Long-term survival	Farahmand *et al.* (2013), Soomro *et al.* (2016), ISTR (2018)
	Obstructive security controls Too secure and decreases effectiveness Hinders business development Workarounds used to avoid security controls	↔	**Supports business innovations** Embedded controls Security balances business needs Focus on resilience	McFadzean *et al.* (2007), Werlinger *et al.* (2009), Kayworth and Whitten (2012), Rothrock *et al.* (2018) Schatz and Bashroush (2018)
Management commitment	**Delegate operations** Security is operational Leads to isolation and insufficient security programmes	↔	**Board commitment** Security is the norm (culture) Legal responsibility	McFadzean *et al.* (2007), Bihari (2008), Johnston and Hale (2009), Kayworth and Whitten (2012) Holgate *et al.* (2012), Barton *et al.* (2016), Soomro *et al.* (2016)
	Technical language Focus on technical details Systems language and systems thinking	↔	**Business language** Message is focused on business risks that impact the strategy	McFadzean *et al.* (2007) Bihari (2008), Farahmand *et al.* (2013), Schinagl and Paans (2017) Haqaf and Koyuncu (2018), Von Solms and Von Solms (2018)

(*continued*)

Table IV.

Tensions	State A: ISG		State B: DSG	References
Interorganisational	**Security is an expense** Minimise protection and maximise compliance Perception that IS investments do not result in direct benefits Security is designed to prevent loss	↔	**Security is an investment** Investments are business enablers Support to "safely" innovate Business agreement on what an acceptable investment means	Soomro *et al.* (2016), Dutta and McCrohan (2002), Schatz and Bashroush (2018), Chulkov (2017), Dreyfuss and Giat (2018)
	Security as a sticking point Fear of losing control Concern regarding trust in vendors Issue of other countries' regulatory environments	↔	**Security as the basis of trust** Control over and trust in partners Holistic approach	Matwyshyn (2009), Rebollo *et al.* (2012), Rebollo *et al.* (2015a), Rebollo *et al.* (2015b), Zapata *et al.* (2017), Dhillon *et al.* (2017), Kemp (2018)
	Poor customer orientation The customer is an under-represented element in the ISG approach	↔	**Customer trust** Transparent about security Earn trust and stay in business	Botsman (2017), Atos (2017), PWC (2017)

approach and include overall business management to act in line with business strategies (Soomro *et al.*, 2016). Such a collaborative approach results in an IS strategy that is more aligned with business goals and that improves security assimilation, e.g. compliance, better policy alignment, the selection of more effective IS security controls and fewer security incidents (Kayworth and Whitten, 2012; Ahmad *et al.*, 2014; Barton *et al.*, 2016; Soomro *et al.*, 2016 Horne *et al.*,2017).

4.1.3 Non-functional security or security embedded by design. Business stakeholders mainly focus on the functionality of new technologies and how to generate value. They care about customer priorities, ease of use, product adoption rates, and legal compliance. Security must contribute value to these priorities. However, the focus often remains on the short-term benefits, e.g. on cheaply and quickly building technologies and products. In this process, security remains non-functional. To illustrate, between 2016 and 2017, the attacks on IoT devices increased by 600 per cent (ISTR, 2018). This shows the vulnerabilities of new technologies and the necessity of developing secure products in the long term. New technologies are often built as cheaply and quickly as possible, not taking security into account "by design". Security cannot be added after an IT environment is deployed (Farahmand *et al.*, 2013); in the digital world, security must be embedded (Soomro *et al.*, 2016).

4.1.4 Obstructive security versus business innovation (the embedding of controls). On the other hand, the penalty of becoming too "secure" is to lose effectiveness and time to market; e.g. security patches decrease the performance of certain applications (Werlinger *et al.*, 2009). Schatz and Bashroush (2018) found that negative user experience with "obstructive" security controls will encourage people to work around them. The requirement to balance the need to increase the functionality of the business against the need to secure information assets is a major challenge (Kayworth and Whitten, 2012). The efforts must not only focus on technological tools (Dreyfuss and Giat, 2018). Instead, the efforts should be to embed the required security controls into the business services such that there is a compromise between business resilience and security, with an emphasis on innovative approaches that enhance the customers' experience (McFadzean *et al.*, 2007; Schatz and Bashroush, 2018). To move at the speed of digitalisation, a business focus on resilience over security becomes even more relevant in DSG (Rothrock *et al.*, 2018).

4.2 Management commitment

IS scholars widely believe that senior executive and board commitment is critical for effective ISG (Veiga and Eloff, 2007; Mukundan and Sai, 2014; Barton *et al.*, 2016; Damenu and Beaumont, 2017). Fortunately, the staggering number of IS breaches (see introduction) has made executives and boards more aware of the need to protect the business and their corporate information assets (Kayworth and Whitten, 2012; Georg, 2017; Von Solms and Von Solms, 2018). However, this level of attention by senior business leaders is relatively new for both executives and security professionals (Schatz and Bashroush, 2018). Therefore, the main tensions in achieving management commitment are defined and discussed in the following sections.

4.2.1 Delegate or commit: why boards and executives are responsible. A major obstacle is convincing boards and executives that they are actually responsible for ISG. Scholars argue that governance is the senior management's primary role in security (Barton *et al.*, 2016). However, there is a continuous debate regarding the role of executives and boards in ISG. Boards see security as "operational" and feel that they are not IT literate enough to take responsibility. They prefer to delegate it to the security specialists in their organisations (McFadzean *et al.*, 2007; Bihari, 2008; Holgate *et al.*, 2012).

In addition to the common argument of being legally responsible for ISG (see the earlier explanation in 3.2.1), devolving security to lower levels not only leads to isolation and insufficient security programmes but also affects the security culture. Johnston and Hale (2009) found that the more active and supportive is the role played by boards and senior executives, the more security-related influence is felt throughout the firm. The result is a culture in which security is the norm rather than the exception and in which security is engrained in the very processes that drive the organisation (Johnston and Hale, 2009).

4.2.2 Communication barriers: technical or business language. The inability of IS experts to express the necessity of ISG leads to poor communication regarding threats and risks and hinders the commitment of management. Scholars have found that IS experts do not have clear arguments about why the board should truly take responsibility (Bihari, 2008). By their nature, experts have a strong interest in operational details and a limited insight into an organisations' business (Farahmand *et al.*, 2013). As the IS discourse used by experts tends to be held in technical language, overusing systems language and systems thinking, many board members find this discourse difficult to engage in (McFadzean *et al.*, 2007; Schinagl and Paans, 2017). The result is that decision makers are not able to make carefully considered risk-based decisions (Schinagl and Paans, 2017). However, the importance of communication skills as part of the key skills needed by IS professionals is underestimated in IS research (Haqaf and Koyuncu, 2018).

If IS professionals want to engage with senior management and boards, the technical message should be redirected. The message should not be about the full scope of IS-related aspects, e.g. physical security, authentication, and logical access. The message should be presented at a level and in a format that is accessible to non-technical corporate directors (Rothrock *et al.*, 2018) and should focus on modern business risks that impact the digital strategy (Von Solms and Von Solms, 2018).

4.2.3 Budgetary constraints: security as an expense or an investment. Another obstacle to engaging senior executives to address security is the difficulty of connecting security expenditures to profitability (Dutta and McCrohan, 2002). Businesses still think of IT security as an expense, not as an investment (Georg, 2017). The evaluation of IS investments, e.g. the tangible return on an IS investment, is complicated by the fact that it is perceived that IS investments do not result in direct financial benefits but are rather designed to prevent losses (Chulkov, 2017; Schatz and Bashroush, 2018). In addition, security measures are viewed as a redundant outlay because security breaches and losses occur despite the investment (Schatz and Bashroush, 2018). This leads to budgetary constraints as an obstacle to ISG (Soomro *et al.*, 2016).

Conventional budgeting approaches (security as an expense) comprise checklist exercises to direct funds towards a "minimum protection/maximum compliance" strategy rather than being initiatives that contribute to the value of the organisation (Dreyfuss and Giat, 2018). Relying heavily on the work of Schatz and Bashroush (2018), we assert that the key principle of IS investments is that they are only seen as business enablers when the selected controls support the businesses to safely innovate, increase market agility, and enhance customer trust. Without appropriately considering the business environment, security programmes will fail to add value. To add value, security controls must be accepted by users and customers. For this to occur, security teams must work with business stakeholders to understand what "acceptable investment" means in a given context.

4.3 From intra- to inter-organisational security

In the digital era, organisations are more collaboratively enabled by technology. In this inter-organisational environment, IS risk crosses boundaries and introduces new forms of

risks by opening opportunities for intrusion, non-compliance and exposure (Karlsson *et al.*, 2016). The tensions derived from the literature related to the inter-organisational perspective are discussed below.

4.3.1 Partners: security as a sticking point or as the basis of trust. Security is perceived as a significant sticking point in establishing a relationship between IT-outsourcing vendors and clients (Zapata *et al.*, 2017; Dhillon *et al.*, 2017; Kemp, 2018). This hinders the trend of adopting vendor-based technologies such as cloud computing (Rebollo *et al.*, 2012). Cloud-computing environments, similar to other outsourcing approaches, provide organisations with great benefits, e.g. approximately 30 per cent more economic savings due to higher productivity and standardisation that support digital business strategies (Rebollo *et al.*, 2015b). However, despite the benefits, it also leads to new organisational risks (Rebollo *et al.*, 2012, Kemp, 2018). The main concern is that cloud computing extends computing resources across the organisation's perimeter, resulting in control being lost over the organisation's information assets (Matwyshyn, 2009; Rebollo *et al.*, 2012; Rebollo *et al.*, 2015a). Dhillon *et al.* (2017) found that one of the highest concerns is trusting that the outsourcing vendor will apply appropriate security controls, especially in the context of different country regulatory environments.

As these new threats need to be managed at a governance level, ISG therefore becomes a process of paramount importance. ISG can help client organisations when they intend to maintain control over cloud services and create trust. ISG is the most suitable path by which to gain control of security processes and to guarantee an alignment with business strategies. ISG frameworks must lead and guide the adoption of technologies such as cloud services; however, the literature in this area is still meagre (Rebollo *et al.*, 2015a; Rebollo *et al.*, 2015b).

4.3.2 Increased reasonable expectations of security by the customer: poor orientation or trust. Technology and digital business activities create a significant change in the way organisations interact with customers. No technology or security strategy will be successful if the customer experience is poor. However, public awareness of today's cyber security threats has grown, and customers' trust in organisations has been decreasing (Botsman, 2017). High-profile incidents have alerted consumers to the potential consequences of their personal information falling into the wrong hands (Atos, 2017).

Today, customers are ready to take their business elsewhere or to ultimately stop using the digital technologies that public sector organisations promote (Atos, 2017; Priisalu and Ottis, 2017; PWC, 2017). Companies must put cyber security and privacy at the forefront of their business strategy to win the customers' hearts and to earn their trust (Atos, 2017). Based on the literature review results, the customer is an under-represented element in the current ISG approaches.

5. Discussion and agenda for further research

The literature review indicates that ISG demands a digital business-oriented approach. ISG approaches should adapt to changing boundaries, i.e. technology-driven organisations that leave no room for distance between security and business (Soomro *et al.*, 2016; Shahim, 2017). Through this lens, most of the relevant practices of ISG potentially lie in disciplines other than IT and security (Bobbert, 2018). Hence, ISG research should broaden its horizons and borrow relevant theories from related research fields. Organisational theories are especially suggested for gaining a deeper understanding of organisational factors that play a role in almost any security breach (Leveson *et al.*, 2009). The following theories are suggested.

5.1 Normal accident and high reliability theory

A possible approach to address the concept of DSG is to focus on organisational factors that play a role in governing security (Leveson *et al.*, 2009). At least two streams of work in organisational theory have addressed organising around high-hazard technologies within organisations: the normal accidents theory (NAT) (Perrow, 1999) and the high reliability theory (HRT) (Weick *et al.*, 2008).

The basic argument of NAT is that the *interactive complexity* and *tight coupling* in some technological systems leads to unpredictability of interactions and hence system accidents that are inevitable or "normal" for these technologies (Perrow, 1999; Leveson *et al.*, 2009 Shrivastava *et al.*, 2009). This clearly shows parallels with security. In today's tightly coupled and highly complex technology-based world, it is not possible to fully predict how an update might create a security vulnerability where none existed before or where one technological behemoth might let the world know a vulnerability exists before a patch is ready (CU*Answers, 2013).

HRT also considers high-risk technologies but focuses on a subset of high-risk organisations, namely, high reliability organisations (HROs). HROs are harbingers of adaptive organisational forms for an increasingly complex environment that strives for error-free performance (Weick *et al.*, 2008; Shrivastava *et al.*, 2009). HROs are characterised by a *preoccupation with failure, a reluctance to simplify interpretations, a sensitivity to operations, a commitment to resilience, and underspecified structur*ing (Weick *et al.*, 2008).

The HRO concept can be illustrative of why so many security failures occur these days. Organisations insufficiently follow HRO principles, including ignoring problems until they grow unavoidable, mistaking security policy/compliance with operational reality, relying on oversimplified risk management tools and security frameworks, and inadequately preparing for security events and incidents. Security studied via HRO characteristics can significantly contribute to the existing research by providing a fundamental understanding of security governance from an organisational perspective (Nash and Hayden, 2016).

5.2 Issue selling and two-factor motivation theory

The literature review indicates that senior management commitment is critical to successful ISG (Veiga and Eloff, 2007; Mukundan and Sai, 2014; Barton *et al.*, 2016; Damenu and Beaumont, 2017). However, the literature that explains how senior managers are motivated to participate in ISG is limited (Barton *et al.*, 2016). By understanding the factors that increase senior management's belief and participation in governing security, ISG can be assimilated in organisations more effectively (Barton *et al.*, 2016). In the context of DSG, *issue selling* is a theory that can be studied and is central to understanding the process in which top management allocates its time and attention to some issues and not to others (Dutton and Ashford, 1993). Issue selling is crucial in this age of rapid change. However, this literature review shows that there are also (communication) barriers to "selling" the importance of security that demand further research.

Additionally, another suggested area of research is the examination of the phenomenon "from the basement to the boardroom" in the context of the motivation theory proposed by Herzberg, known as the two-factor theory of job satisfaction (Herzberg, 1968). The concept and assumptions of this theory can be applied to structure the shift from the ISG phenomenon towards DSG. For example, the traditional factors of ISG, e.g. strategy, laws and regulation, risk management, resources and operations, are dissatisfiers (hygiene factors). These factors are necessary; for example, organisations are required to comply with laws and regulation. However, this literature review shows that this approach is insufficient in meeting the current IS challenge and that these factors are not the ones that "motivate"

the organisation to develop an IS strategy or to bring security to a higher level. To increase the professionalism of security within the organisation, further clarity needs to be provided on the relationship between security satisfiers and the DSG construct.

6. Implications

The objective of this study is to examine and structure the ISG literature. We have fulfilled this objective by emphasising the tensions that exist at the intersection of the rapidly changing business climate and the current body of knowledge in ISG. The originality of the paper is mainly demonstrated by providing a novel "digital lens" for studying and further understanding the ISG concept in the current digital era.

6.1 Implications for practice

Accordingly, this research has implications for practice because "digital" is currently one of hottest buzzwords (Büyüközkan and Göçer, 2018). The findings of this paper show that within the digital context, security must be seen as an indispensable feature. This paper supports practitioners and decision makers by providing a deeper understanding of how organisations and their security approaches are actually affected by digitalisation. As they continue to confront the discussed tensions and begin to embrace the principles of "Digital Security Governance", organisations can start adapting their current security approaches. We believe that our research findings are especially useful in helping practitioners and senior executives understand that DSG is not an excessive technical issue that hinders business goals. Instead, DSG is about pursuing resilient approaches that support digital business strategies and business innovation (Holgate *et al.*, 2012; Williams *et al.*, 2013; Tan *et al.*, 2017; Nicho, 2018; Rothrock *et al.*, 2018).

6.2 Implications for research

The concept of DSG is a new research territory that addresses the limitations and gaps of traditional ISG approaches in a digital context (see tensions in Table IV). To this extent, theories are suggested that to the knowledge of the authors have not yet been discovered in IS research. Doing so will help build knowledge that offers a deeper understanding than that provided by the too often used practical approaches in ISG research. In addition, the line of reasoning in this paper, i.e. the impact of the digital context on specific areas and a stronger theoretical grounding by borrowing theories from related fields, should be taken in a wider sense and is also relevant for other IS research areas and beyond, e.g. customer orientation in ISG approaches, communication barriers between IS experts and decision makers and especially the theoretical relation to other governance domains that are not included in this scope (internet, data, network and e-governance).

6.3 Implications for society

Because digitalisation has touched almost every aspect of human life all over the world (Büyüközkan and Göçer, 2018), there are also implications for society. Participating in this technologically driven world means dealing not only with great benefits but also with potential risks. People in this risky environment have to be aware of how this digital change impacts them. This paper helps individuals understand that they have increasing rights with regards to privacy and security and a say in what parties they do business with. We argue that people still often make decisions based on the functionalities of services instead of making critical privacy- and security-considered decisions when doing business. An

increased awareness with regard to this external force can be very beneficial in stimulating organisations to transparently govern security.

7. Concluding remarks

Our literature review shows that security has shifted from a narrow-focused isolated issue towards a strategic business issue with "from the basement to the boardroom" implications. Tensions are identified and considered "gaps" that occur between DSG and the current common body of knowledge in ISG. We believe that, by studying ISG through a "digital lens", we have challenged underlying assumptions that lead to the introduction of the DSG concept. Our key takeaway is that protecting the organisation is important, but organizations must also develop strategies to ensure resilient businesses to take advantage of the opportunities that digitalization can bring.

References

Ahmad, A., Maynard, S.B. and Park, S. (2014), "Information security strategies: towards an organizational multi-strategy perspective", *Journal of Intelligent Manufacturing*, Vol. 25 No. 2, pp. 357-370, doi: 10.1007/s10845-012-0683-0.

Alavi, R., Islam, S. and Mouratidis, H. (2016), "An information security risk-driven investment model for analysing human factors", *Information and Computer Security*, Vol. 24 No. 2, pp. 205-227, doi: 10.1108/ICS-01-2016-0006.

Atos (2017), "The currency of cyber trust: your customers' attitudes towards cyber security", available at: https://atos.net/wp-content/uploads/2018/03/atos-currency-cyber-truth-research-programme-report.pdf

Barton, K.A., Tejay, G., Lane, M. and Terrell, S. (2016), "Information system security commitment: a study of external influences on senior management", *Computers and Security*, Vol. 59, pp. 9-25, doi: 10.1016/j.cose.2016.02.007.

Berkman, H., Jona, J., Lee, G. and Soderstrom, N. (2018), "Cybersecurity awareness and market valuations", *Journal of Accounting and Public Policy*, Vol. 37 No. 6, pp. 508-526, doi: 10.1016/j.jaccpubpol.2018.10.003.

Bihari, E. (2008), "Information security governance and boards of directors: are they compatible?", *Proceedings of the 6th Australian Information Security Management Conference*, Edith Cowan University, Perth, 1st to 3rd December 2008, doi: 10.4225/75/57b5595fb8768.

Bobbert, Y. (2018), *Improving the Maturity of Business Information Security*, Radboud University Nijmegen in partnership with University of Antwerp, Datawyse | Universitaire Pers Maastricht, Maastricht.

Botsman, R. (2017), *Who Can You Trust?: How Technology Brought Us Together and Why It Might Drive Us Apart*, Penguin Random House, UK.

Büyüközkan, G. and Göçer, F. (2018), "Digital supply chain: literature review and a proposed framework for future research", *Computers in Industry*, Vol. 97, pp. 157-177.

Carcary, M., Renaud, K., McLaughlin, S. and O'Brien, C. (2016), "A framework for information security governance and management", *IT Professional*, Vol. 18 No. 2, pp. 22-30, available at: https://doi.ieeecomputersociety.org/10.1109/MITP.2016.27

Chulkov, D.V. (2017), "Escalation of commitment and information security: theories and implications", *Information and Computer Security*, Vol. 25 No. 5, pp. 580-592, doi: 10.1108/ICS-02-2016-0015.

Cram, W.A., Proudfoot, J.G. and D'Arcy, J. (2017), "Organizational information security policies: a review and research framework", *European Journal of Information Systems*, Vol. 26 No. 6, pp. 605-641, doi: 10.1057/s41303-017-0059-9.

CU*Answers (2013), "Sense and reliability: do we have the right approach to risk management for our future – especially when it comes to cyber security?", available at: www.cuanswers.com/wp-content/uploads/Cybersecurity-WhitePaper-SenseandReliability.pdf

Da Veiga, A. and Martins, N. (2015), "Improving the information security culture through monitoring and implementation actions illustrated through a case study", *Computers and Security*, Vol. 49, pp. 162-176, doi: 10.1016/j.cose.2014.12.006.

Damenu, T.K. and Beaumont, C. (2017), "Analysing information security in a bank using soft systems methodology", *Information and Computer Security*, Vol. 25 No. 3, pp. 240-258, doi: 10.1108/ICS-07-2016-0053.

Dang-Pham, D., Pittayachawan, S. and Bruno, V. (2017), "Applications of social network analysis in behavioural information security research: concepts and empirical analysis", *Computers and Security*, Vol. 68, pp. 1-15, doi: 10.1016/j.cose.2017.03.010.

Dhillon, G., Syed, R. and de Sá-Soares, F. (2017), "Information security concerns in IT outsourcing: identifying (in) congruence between clients and vendors", *Information and Management*, Vol. 54 No. 4, pp. 452-464, doi: 10.1016/j.im.2016.10.002.

Dreyfuss, M. and Giat, Y. (2018), "A risk management model for an academic institution's information system", *Information Resources Management Journal (Journal*,), Vol. 31 No. 1, pp. 83-96, doi: 10.4018/IRMJ.2018010104.

Dutta, A. and McCrohan, K. (2002), "Management's role in information security in a cyber economy", *California Management Review*, Vol. 45 No. 1, pp. 67-87, doi: 10.2307/41166154.

Dutton, J.E. and Ashford, S.J. (1993), "Selling issues to top management", *Academy of Management Review*, Vol. 18 No. 3, pp. 397-428, doi: 10.5465/amr.1993.9309035145.

Farahmand, F., Atallah, M.J. and Spafford, E.H. (2013), "Incentive alignment and risk perception: an information security application", *IEEE Transactions on Engineering Management*, Vol. 60 No. 2, pp. 238-246, doi: 10.1109/TEM.2012.2185801.

Flores, W.R., Antonsen, E. and Ekstedt, M. (2014), "Information security knowledge sharing in organizations: investigating the effect of behavioral information security governance and national culture", *Computers and Security*, Vol. 43, pp. 90-110, doi: 10.1016/j.cose.2014.03.004.

Georg, L. (2017), "Information security governance: pending legal responsibilities of non-executive boards", *Journal of Management and Governance*, Vol. 21 No. 4, pp. 793-814, doi: 10.1007/s10997-016-9358-0.

Gillon, K., Branz, L., Culnan, M.J., Dhillon, G., Hodgkinson, R. and MacWillson, A. (2011), "Information security and privacy-rethinking governance models", *Communications of the Association for Information Systems*, Vol. 28, p. 33, doi: 10.17705/1CAIS.02833.

Goel, S. and Shawky, H.A. (2009), "Estimating the market impact of security breach announcements on firm values", *Information and Management*, Vol. 46 No. 7, pp. 404-410, doi: 10.1016/j.im.2009.06.005.

Haqaf, H. and Koyuncu, M. (2018), "Understanding key skills for information security managers", *International Journal of Information Management*, Vol. 43, pp. 165-172, doi: 10.1016/j.ijinfomgt.2018.07.013.

Hasbini, M.A., Eldabi, T. and Aldallal, A. (2018), "Investigating the information security management role in smart city organisations", *World Journal of Entrepreneurship, Management and Sustainable Development*, Vol. 14 No. 1, pp. 86-98, doi: 10.1108/WJEMSD-07-2017-0042.

Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K. and Stantchev, V. (2016), "A process framework for information security management", *International Journal of Information Systems and Project Management*, Vol. 4 No. 4, pp. 27-47, doi: 10.12821/ijispm040402.

Herzberg, F. (1968), "One more time: how do you motivate employees?", *Harvard Business Review*, Vol. 46 (January), pp. 53-62.

Higgs, J.L., Pinsker, R.E., Smith, T.J. and Young, G.R. (2016), "The relationship between board-level technology committees and reported security breaches", *Journal of Information Systems*, Vol. 30 No. 3, pp. 79-98, doi: 10.2308/isys-51402.

Holgate, J.A., Williams, S.P. and Hardy, C.A. (2012), "Information security governance: investigating diversity in critical infrastructure organizations", Bled proceedings, p. 13, available at: https://aisel.aisnet.org/bled2012/13

Horne, C.A., Maynard, S.B. and Ahmad, A. (2017), "Organisational information security strategy: review, discussion and future research", *Australasian Journal of Information Systems*, Vol. 21, doi: 10.3127/ajis.v21i0.1427.

ISTR (2018), "Information Security Threat Report (ISTR)", Vol. 23, Symantec, available at: www.symantec.com/security-center/threat-report

Johnston, A.C. and Hale, R. (2009), "Improved security through information security governance", *Communications of the ACM*, Vol. 52 No. 1, pp. 126-129, doi: 10.1145/1435417.1435446.

Karanja, E. (2017), "The role of the chief information security officer in the management of IT security", *Information and Computer Security*, Vol. 25 No. 3, pp. 300-329, doi: 10.1108/ICS-02-2016-0013.

Karlsson, F., Kolkowska, E. and Prenkert, F. (2016), "Inter-organisational information security: a systematic literature review", *Information and Computer Security*, Vol. 24 No. 5, pp. 418-451, doi: 10.1108/ICS-11-2016-091.

Kauspadiene, L., Cenys, A., Goranin, N., Tjoa, S. and Ramanauskaite, S. (2017), "High-level self-sustaining information security management framework", *Baltic Journal of Modern Computing*, Vol. 5 No. 1, p. 107, doi: 10.22364/bjmc.2017.5.1.07.

Kayworth, K.T. and Whitten, D. (2012), "Effective information security requires a balance of social and technology factors", *MIS Quarterly Executive*, Vol. 9 No. 3, pp. 2012-2052, Mays Business School Research Paper No. 2012-52, SSRN available at: https://ssrn.com/abstract=2058035

Kemp, R. (2018), "Legal aspects of cloud security", *Computer Law and Security Review*, Vol. 34 No. 4, pp. 928-932, doi: 10.1016/j.clsr.2018.06.001.

Knapp, K.J., Morris, R.F., Jr, Marshall, T.E. and Byrd, T.A. (2009), "Information security policy: an organizational-level process model", *Computers and Security*, Vol. 28 No. 7, pp. 493-508, doi: 10.1016/j.cose.2009.07.001.

Leveson, N., Dulac, N., Marais, K. and Carroll, J. (2009), "Moving beyond normal accidents and high reliability organizations: a systems approach to safety in complex systems", *Organization Studies*, Vol. 30 Nos 2/3, pp. 227-249, doi: 10.1177/0170840608101478.

Lindup, K. (1996), "The role of information security in corporate governance", *Computers and Security*, Vol. 15 No. 6, pp. 477-485, doi: 10.1016/S0167-4048(97)83121-5.

McFadzean, E., Ezingeard, J.N. and Birchall, D. (2007), "Perception of risk and the strategic impact of existing IT on information security strategy at board level", *Online Information Review*, Vol. 31 No. 5, pp. 622-660, doi: 10.1108/14684520710832333.

Maleh, Y., Ezzati, A., Sahid, A. and Belaissaoui, M. (2017), "CAFISGO: a capability assessment framework for information security governance in organizations", *Journal of Information Assurance and Security*, Vol. 12 No. 6, pp. 209-217.

Matwyshyn, A.M. (2009), "CSR and the corporate cyborg: ethical corporate information security practices", *Journal of Business Ethics*, Vol. 88, pp. 579-594, doi: 10.1007/s10551-009-0312-9.

Maynard, S.B., Tan, T., Ahmad, A. and Ruighaver, T. (2018), "Towards a framework for strategic security context in information security governance", *Pacific Asia Journal of the Association for Information Systems*, Vol. 10 No. 4, doi: 10.17705/1pais.10403.

Mishra, S. (2015), "Organizational objectives for information security governance: a value focused assessment", *Information and Computer Security*, Vol. 23 No. 2, pp. 122-144, doi: 10.1108/ICS-02-2014-0016.

Moghadam, R.S. and Colomo-Palacios, R. (2018), "Information security governance in big data environments: a systematic mapping", *Procedia Computer Science*, Vol. 138, pp. 401-408, doi: 10.1016/j.procs.2018.10.057.

Moulton, R. and Coles, R.S. (2003), "Applying information security governance", *Computers and Security*, Vol. 22 No. 7, pp. 580-584, doi: 10.1016/S0167-4048(03)00705-3.

Mukundan, N.R. and Sai, L.P. (2014), "Perceived information security of internal users in Indian IT services industry", *Information Technology and Management*, Vol. 15 No. 1, pp. 1-8, doi: 10.1007/s10799-013-0156-y.

Nash, C. and Hayden, L. (2016), "What high reliability organizations can teach us about security", available at: www.oreilly.com/ideas/what-high-reliability-organizations-can-teach-us-about-security (13 September 2016).

Nicho, M. (2018), "A process model for implementing information systems security governance", *Information and Computer Security*, Vol. 26 No. 1, pp. 10-38, doi: 10.1108/ICS-07-2016-0061.

Ozkan, S. and Karabacak, B. (2010), "Collaborative risk method for information security management practices: a case context within Turkey", *International Journal of Information Management*, Vol. 30 No. 6, pp. 567-572, doi: 10.1016/j.ijinfomgt.2010.08.007.

Park, H., Kim, S. and Lee, H.J. (2006), "General drawing of the integrated framework for security governance", *International Conference on Knowledge-Based and Intelligent Information and Engineering Systems, LNCS*, Vol. 4251, Springer, Berlin, Heidelberg, pp. 1234-1241.

Perrow, C. (1999), *Normal Accidents: Living with High-Risk Technologies*, 2nd ed., Princeton University Press, Princeton, NJ.

Posthumus, S. and Von Solms, R. (2004), "A framework for the governance of information security", *Computers and Security*, Vol. 23 No. 8, pp. 638-646, doi: 10.1016/j.cose.2004.10.006.

Priisalu, J. and Ottis, R. (2017), "Personal control of privacy and data: Estonian experience", *Health and Technology*, Vol. 7 No. 4, pp. 441-451, doi: 10.1007/s12553-017-0195-1.

PWC (2017), "Consumer intelligence series: Protect.me, an in-depth look at what consumers want, what worries them, and how companies can earn their trust – and their business", available at: www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf

Rebollo, O., Mellado, D. and Fernández-Medina, E. (2012), "A systematic review of information security governance frameworks in the cloud computing environment", *J. Ucs*, Vol. 18 No. 6, pp. 798-815, doi: 10.3217/jucs-018-06-0798.

Rebollo, O., Mellado, D. and Fernandez-Medina, E. (2015a), "ISGcloud: a security governance framework for cloud computing", *The Computer Journal*, Vol. 58 No. 10, pp. 2233-2254, doi: 10.1093/comjnl/bxu141.

Rebollo, O., Mellado, D., Fernández-Medina, E. and Mouratidis, H. (2015b), "Empirical evaluation of a cloud computing information security governance framework", *Information and Software Technology*, Vol. 58, pp. 44-57, doi: 10.1016/j.infsof.2014.10.003.

Romansky, R. (2017), "A survey on digital world opportunities and challenges for user's privacy", *International Journal on Information Technologies and Security (Bulgaria)*, Vol. 4 No. 9, pp. 97-112.

Rothrock, R.A., Kaplan, J. and Van, D.O. (2018), "The board's role in managing cybersecurity risks", *MIT Sloan Management Review*, Vol. 59 No. 2, pp. 12-15, available at: https://search-proquest-com.vu-nl.idm.oclc.org/docview/–1986317468?accountid=10978

Ruighaver, A.B., Maynard, S.B. and Chang, S. (2007), "Organisational security culture: extending the end-user perspective", *Computers and Security*, Vol. 26 No. 1, pp. 56-56, doi: 10.1016/j.cose.2006.10.008.

Schatz, D. and Bashroush, R. (2017), "Economic valuation for information security investment: a systematic literature review", *Information Systems Frontiers*, Vol. 19 No. 5, pp. 1205-1228, doi: 10.1007/s10796-016-9648-8.

Schatz, D. and Bashroush, R. (2018), "Corporate information security investment decisions: a qualitative data analysis approach", *International Journal of Enterprise Information Systems (Systems)*, Vol. 14 No. 2, pp. 1-20, doi: 10.4018/IJEIS.2018040101.

Schinagl, S. and Paans, R. (2017), "Communication barriers in the decision-making process: system language and system thinking", *Proceedings of the 50th HI International Conference on System Sciences*, available at: http://hdl.handle.net/10125/41902

Shahim, A. (2017), *Think Technology: Towards an Orientation of IT Auditing*, Vrije Universiteit Amsterdam, IT-audit, compliance and advisory, Amsterdam, available at: https://sbe.vu.nl/nl/nieuws-agenda/agenda/2017/okt-dec/06dec_profdring-a-shahim.aspx#.XUnU1-gzaUk

Shrivastava, S., Sonpar, K. and Pazzaglia, F. (2009), "Normal accident theory versus high reliability theory: a resolution and call for an open systems view of accidents", *Human Relations*, Vol. 62 No. 9, pp. 1357-1390, doi: 10.1177/0018726709339117.

Siponen, M. and Willison, R. (2009), "Information security management standards: problems and solutions", *Information and Management*, Vol. 46 No. 5, pp. 267-270, doi: 10.1016/j.im.2008.12.007.

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016), "Information security management needs more holistic approach: a literature review", *International Journal of Information Management*, Vol. 36 No. 2, pp. 215-225, doi: 10.1016/j.ijinfomgt.2015.11.009.

Stewart, H. and Jürjens, J. (2017), "Information security management and the human aspect in organizations", *Information and Computer Security*, Vol. 25 No. 5, pp. 494-534, doi: 10.1108/ICS-07-2016-0054.

Tan, T., Maynard, S., Ahmad, A. and Ruighaver, T. (2017), "Information security governance: a case study of the strategic context of information security", PACIS 2017 Proceedings, p. 43, available at: https://aisel.aisnet.org/pacis2017/43

Thomson, K.L. and Von Solms, R. (2005), "Information security obedience: a definition", *Computers and Security*, Vol. 24 No. 1, pp. 69-75, doi: 10.1016/j.cose.2004.10.005.

Veale, M., Binns, R. and Edwards, L. (2018), "Algorithms that remember: model inversion attacks and data protection law", *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, Vol. 376 No. 2133, doi: 10.1098/rsta.2018.0083.

Veiga, A.D. and Eloff, J.H. (2007), "An information security governance framework", *Information Systems Management*, Vol. 24 No. 4, pp. 361-372, doi: 10.1080/10580530701586136.

Von Solms, B. (2001a), "Corporate governance and information security", *Computers and Security*, Vol. 20 No. 3, pp. 215-218.

Von Solms, B. (2001b), "Information security – a multidimensional discipline", *Computers and Security*, Vol. 20 No. 6, pp. 504-508.

Von Solms, B. (2005), "Information security governance: COBIT or ISO 17799 or both?", *Computers and Security*, Vol. 24 No. 2, pp. 99-104, doi: 10.1016/j.cose.2005.02.002.

Von Solms, B. (2006), "Information security–the fourth wave", *Computers and Security*, Vol. 25 No. 3, pp. 165-168, doi: 10.1016/j.cose.2006.03.004.

Von Solms, B. and Von Solms, R. (2005), "From information security too business security?", *Computers and Security*, Vol. 24 No. 4, pp. 271-273, doi: 10.1016/j.cose.2005.04.004.

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, doi: 10.1108/ICS-04-2017-0025.

Von Solms, V. and Von Solms, B. (2006a), "Information security governance: a model based on the direct–control cycle", *Computers and Security*, Vol. 25 No. 6, pp. 408-412, doi: 10.1016/j.cose.2006.07.005.

Von Solms, R. and von Solms, S.B. (2006b), "Information security governance: due care", *Computers and Security*, Vol. 25 No. 7, pp. 494-497, doi: 10.1016/j.cose.2006.08.013.

Weick, K.E., Sutcliffe, K.M. and Obstfeld, D. (2008), "Organizing for high reliability: processes of collective mindfulness", in Sutton, R.I. and Staw, B.M. (Eds), *Research in Organizational Behavior*, Elsevier Science/JAI Press, Vol. 21, pp. 81-123.

Werlinger, R., Hawkey, K. and Beznosov, K. (2009), "An integrated view of human, organizational, and technological challenges of IT security management", *Information Management and Computer Security*, Vol. 17 No. 1, pp. 4-19, doi: 10.1108/09685220910944722.

Williams, S.P., Hardy, C.A. and Holgate, J.A. (2013), "Information security governance practices in critical infrastructure organizations: a socio-technical and institutional logic perspective", *Electronic Markets*, Vol. 23 No. 4, pp. 341-354, doi: 10.1007/s12525-013-0137-3.

Wu, A. and Saunders, C.S. (2016), "Governing the fiduciary relationship in information security services", *Decision Support Systems*, Vol. 92, pp. 57-67, doi: 10.1016/j.dss.2016.09.008.

Zafar, H. and Clark, J.G. (2009), "Current state of information security research in IS", *Communications of the Association for Information Systems*, Vol. 24 No. 1, p. 34, doi: 10.17705/1CAIS.02434.

Zapata, B.C., Fernández-Alemán, J.L. and Toval, A. (2017), "Security in cloud computing: a mapping study", *Computer Science and Information Systems*, Vol. 12 No. 1, pp. 161-184, doi: 10.2298/CSIS140205086C.

Further reading

Herzberg, F., Mausner, B. and Snyderman, B.B. (1993), *The Motivation to Work*, Transaction Publishers, New Brunswick, NJ, available at: https://trove.nla.gov.au/version/43147719

Corresponding author

Stef Schinagl can be contacted at: s.schinagl@vu.nl

Reference	Theoretical construct	State of research	Empirical or conceptual	Qualitative/ quantitative	Methodology
Ahmad *et al.* (2014)	IS strategy	Theory generating	Empirical	Qualitative	Focus groups
Alavi *et al.* (2016)	IS investment	Theoretical	Conceptual	Mixed method	Brainstorm sessions and survey
Barton *et al.* (2016)	Neo-institutional theory	Theory testing	Empirical	Quantitative	Survey
Berkman *et al.* (2018)	IS investment	Theory testing	Empirical	Quantitative	Cybersecurity awareness measures (SCORE)
Bihari (2008)	Agency theory	Theory generating	Empirical	Qualitative	Delphi method
Büyüközkan and Göçer (2018)	Digital supply chain	Theoretical	Conceptual	–	Literature review
Carcary *et al.* (2016)	ISG management	Descriptive	Conceptual	–	–
Chulkov (2017)	Escalation of commitment	Theoretical	Conceptual	–	Literature review
Cram *et al.* (2017)	IS policies	Theoretical	Conceptual	–	Literature review
Veiga and Eloff (2007)	IS culture	Descriptive	Conceptual	–	Comparison four practical standards
Da Veiga and Martins (2015)	IS culture	Theory generating	Empirical	Quantitative	Case study, survey
Damenu and Beaumont (2017)	Soft system methodology	Theory generating	Empirical	Qualitative	Single case study, semi-structured interviews
Dang-Pham *et al.* (2017)	Social network analyses	Theory generating	Empirical	Qualitative	Case study
Dhillon *et al.* (2017)	IT-outsourcing	Theory generating	Empirical	Qualitative	Delphi method
Dreyfuss and Giat (2018)	IS investment	Theory generating	Empirical	Quantitative	Case study
Dutta and McCrohan (2002)	–	Philosophical	Conceptual	Qualitative	–
Farahmand *et al.* (2013)	Risk perception and incentive	Theory generating	Empirical	Qualitative	Interviews
Flores *et al.* (2014)	Knowledge sharing	Theory testing	Empirical	Mixed method	Survey and interviews
Georg (2017)	Corporate governance	Theory generating	Empirical	Qualitative	Single case study

(*continued*)

Table AI.
Detailed analysis

Table AI.

Reference	Theoretical construct	State of research	Empirical or conceptual	Qualitative/ quantitative	Methodology
Gillon *et al.* (2011)	ISG	Descriptive	Conceptual	–	Opinion paper, panel discussion
Goel and Shawky (2009)	IS investment	Theory generating	Empirical	Quantitative	Event-study methodology
Haqaf and Koyuncu (2018)	IS management	Theory generating	Empirical	Qualitative	Delphi method
Hasbini *et al.* (2018)	Smart cities	Descriptive	Conceptual	–	Literature review
Haufe *et al.* (2016)	None	Theory generating	Empirical	Pilot	–
Higgs *et al.* (2016)	Signalling theory	Theory testing	Empirical	Quantitative	Analysis on breach samples
Holgate *et al.* (2012)	ISG	Theory generating	Empirical	Qualitative	Multiple case study
Horne *et al.* (2017)	IS strategy	Philosophical	Conceptual	–	Literature review
Johnston and Hale (2009)	ISG	Theory generating	Empirical	Quantitative	Survey
Karanja (2017)	Agency theory	Theoretical	Conceptual	Qualitative	Analysis on breach samples
Karlsson *et al.* (2016)	Inter-organizational security	Theoretical	Conceptual	–	Literature review
Kauspadiene *et al.* (2017)	None	Descriptive	Conceptual	–	Comparison of ISG-models
Kayworth and Whitten (2012)	IS strategy	Theory generating	Empirical	Qualitative	Interviews
Kemp (2018)	ISG (Cloud)	Descriptive	Conceptual	–	Checklist
Knapp *et al.* (2009)	Grounded theory	Theory generating	Empirical	Qualitative	Open-ended questions
Lindup (1996)	ISG	Descriptive	Conceptual	–	Opinion paper
Maleh *et al.* (2017)	ISG	Theory generating	Empirical	Qualitative	Case study, questionnaire
Matwyshyn (2009)	Business ethics in the context of corporate IS	Philosophical	Conceptual	–	–
Maynard *et al.* (2018)	ISG	Theory generating	Conceptual	Qualitative	Case study
McFadzean *et al.* (2007)	Grounded theory need theory	Theory generating	Empirical	Qualitative	Interviews
Mishra (2015)	Value-focused thinking	Theory generating	Empirical	Qualitative	Interviews

(*continued*)

Table AI.

Reference	Theoretical construct	State of research	Empirical or conceptual	Qualitative/ quantitative	Methodology
Moghadam and Colomo-Palacios (2018)	ISG (big data)	Theoretical	Conceptual	–	Literature review
Moulton and Coles (2003)	ISG	Descriptive	Conceptual	–	–
Mukundan and Sai (2014)	Perceived information security	Theory generating	Empirical	Quantitative	Survey
Nicho (2018)	ISG	Theory generating	Empirical	Qualitative	Interviews
Ozkan and Karabacak (2010)	collaborative risk method	Theoretical	Conceptual	Qualitative	Case study
Park *et al.* (2006)	ISG	Descriptive	Conceptual	–	–
Posthumus and von Solms (2004)	ISG	Descriptive	Conceptual	–	–
Priisalu and Ottis (2017)	Information security and privacy	Theoretical	Conceptual	–	–
Rebollo *et al.* (2012)	ISG (Cloud)	Theoretical	Conceptual	–	Literature review
Rebollo *et al.* (2015a)	ISG (Cloud)	Descriptive	Conceptual	–	–
Rebollo *et al.* (2015b)	ISG (Cloud)	Theory generating	Empirical	Quantitative	Case study
Romansky (2017)	–	Philosophical	Conceptual	–	–
Rothrock *et al.* (2018)	Digital Security Governance	Descriptive	Conceptual	–	–
Ruighaver *et al.* (2007)	IS culture	Theoretical	Conceptual	–	–
Schatz and Bashroush (2018)	Grounded theory-IS investment decisions	Theory generating	Empirical	Qualitative	Semi-structured interviews
Schatz and Bashroush (2017)	IS investment	Theoretical	Conceptual	–	Literature review
Siponen and Willison (2009)	IS management	Descriptive	Conceptual	–	Comparison of ISG-models
Soomro *et al.* (2016)	IS management	Theoretical	Conceptual	–	Literature Review

(*continued*)

Table AI.

Reference	Theoretical construct	State of research	Empirical or conceptual	Qualitative/ quantitative	Methodology
Stewart and Jürjens (2017)	Information security	Theory generating	Empirical	Quantitative	Survey
Tan *et al.* (2017)	Enterprise wide ISG	Theoretical	Conceptual	Quantitative	Case study
Thomson and von Solms (2005)	IS obedience	Descriptive	Conceptual	–	–
Veale *et al.* (2018)	Governing artificial intelligence	Theoretical	Conceptual	–	Probing Experiment
Von Solms and Von Solms (2005)	ISG	Descriptive	Conceptual	–	–
Von Solms and Von Solms (2005)	ISG	Philosophical	Conceptual	–	–
von Solms and von Solms (2006a)	ISG	Descriptive	Conceptual	–	–
von Solms and von Solms (2006b)	Due care	Theoretical	Conceptual	–	–
von Solms and von Solms (2018)	ISG	Philosophical	Conceptual	–	Desk research
Von Solms (2001a)	ISG	Philosophical	Conceptual	–	–
Von Solms (2001b)	ISG	Descriptive	Conceptual	–	–
von Solms (2005)	ISG	Descriptive	Conceptual	–	–
Von Solms (2006)	ISG	Descriptive	Conceptual	–	–
Werlinger *et al.* (2009)	IS management	Theory generating	Empirical	Qualitative	Semi-structured interviews
Williams *et al.* (2013)	ISG	Theory generating	Empirical	Qualitative	Case study
Wu and Saunders (2016)	Agency theory	Theory testing	Empirical	Quantitative	Survey
Zafar and Clark (2009)	IS research	Theoretical	Conceptual	–	–
Zapata *et al.* (2017)	ISG (Cloud)	Theoretical	Conceptual	–	Mapping-study