A quantification mechanism for assessing adherence to information security governance guidelines

Ivano Bongiovanni
The University of Queensland, Brisbane, Australia

Karen Renaud
Department of Computer and Information Sciences, University of Strathclyde, Glasgow, UK and Information Systems, Rhodes University, Grahamstown, South Africa

Humphrey Brydon and Renette Blignaut
University of the Western Cape, Cape Town, South Africa, and

Angelo Cavallo
Politecnico di Milano, Milan, Italy

Received 10 August 2021
Revised 10 November 2021
6 December 2021
13 January 2022
Accepted 16 January 2022

Abstract

Purpose – Boards of Directors and other organisational leaders make decisions about the information security governance systems to implement in their companies. The increasing number of cyber-breaches targeting businesses makes this activity inescapable. Recently, researchers have published comprehensive lists of recommended cyber measures, specifically to inform organisational boards. However, the young cybersecurity industry has still to confirm and refine these guidelines. As a starting point, it would be helpful for organisational leaders to know what other organisations are doing in terms of using these guidelines. In an ideal world, bespoke surveys would be developed to gauge adherence to guidelines, but this is not always feasible. What we often do have is data from existing cybersecurity surveys. The authors argue that such data could be repurposed to quantify adherence to existing information security guidelines, and this paper aims to propose, and test, an original methodology to do so.

Design/methodology/approach – The authors propose a quantification mechanism to measure the degree of adherence to a set of published information security governance recommendations and guidelines targeted at organisational leaders. The authors test their quantification mechanism using a data set collected in a survey of 156 Italian companies on information security and privacy.

Findings – The evaluation of the proposed mechanism appears to align with findings in the literature, indicating the validity of the present approach. An analysis of how different industries rank in terms of their adherence to the selected set of recommendations and guidelines confirms the usability of our repurposed data set to measure adherence.

Originality/value – To the best of the authors' knowledge, a quantification mechanism as the one proposed in this study has never been proposed, and tested, in the literature. It suggests a way to repurpose survey data to determine the extent to which companies are implementing measures recommended by

This research did not receive any specific grant from funding agencies in the public, commercial or not-for-profit sectors. The authors also declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Information & Computer Security
Vol. 30 No. 4, 2022
pp. 517-548

2056-4961
DOI 10.1108/ICS-08-2021-0112

published cybersecurity guidelines. This way, the proposed mechanism responds to increasing calls for the adoption of research practices that minimise waste of resources and enhance research sustainability.

Keywords Survey, Boards of Directors, Information security governance, Cybersecurity, Adherence quantification mechanism, Information security guidelines, Organisational leaders

Paper type Research paper

1. Introduction

In a COVID19 world, companies are experiencing unprecedented pressure on their diminished finances. At the same time, their need for protection from external threats is growing, as cyber-attacks escalate worldwide (Sobers, 2021). Information security decisions are therefore more important than ever. Organisational Boards of Directors (BoDs), including those who do not have an information security background, make decisions around investments in this field. This ensures that the organisation's approach to information security is proactive and strategic (Rothrock *et al.*, 2018).

Defined as "a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organizational resources responsibly, and monitors the success or failure of the enterprise security program" (IT Governance Institute, 2006, p. 11), information security governance operationalises the need for organisations to align security processes with business strategies (Rebollo *et al.*, 2015). Security solutions, such as the setup of a Security Operations Centre, or reliance on outsourced security, are impacted by factors such as maturity, size and industry of the organisation, budget availability and legal requirements. Selecting the most appropriate solutions is challenging, especially when decision-makers are not experts in the field. For example, deciding how much to spend on information security is particularly daunting (Teplinsky, 2013).

Given this difficulty, BoDs are likely to prioritise spending based on data about the effectiveness of different information security measures. The problem is that there is a lack of hard evidence to inform such prioritisation. The overall picture is complicated by a lack of agreement, even between experts, on the key constituents of an effective information security governance programme. In particular, there is often disagreement about which measures are essential, which are advisable and which are *nice to have* (Redmiles *et al.*, 2020).

Researchers have published guidelines specifically for the benefit of BoDs, executives and top management (Renaud *et al.*, 2019; Zukis, 2016). Because organisations engage in social comparisons with their peers to decide which measures to implement (Barlette *et al.*, 2017), it would be helpful for organisational leaders to have an indication of the extent to which such peers adhere (or do not adhere) to recommended information security governance guidelines, based on agreed upon measurement mechanisms. Governments, too, would find it useful to have an awareness of how the companies in their country are managing cybersecurity. The UK government, for example, collects data about cyber breaches every year (UK Government, 2020). It might be possible to use this data to gauge the extent to which the surveyed companies have followed recommended guidelines.

In an era of scarcity of resources, pressures towards the sustainable conduct of research are increasing. Among others, recent work (Ligozat *et al.*, 2020) has encouraged the re-use of existing research materials, as long as pertinent to the addressed research questions, to limit the waste of research resources. After all, novelty does not come only from new data sets, but also from the application of existing data sets to new contexts. This can, furthermore, demonstrate reproducibility, another cornerstone of sustainable research practices.

Learning from these lessons, to facilitate repurposing of existing information security data, we formulated a quantification mechanism that can be used to evaluate businesses' adherence to the framework of information security governance guidelines proposed by Renaud *et al.* (2019). We tested our mechanism by repurposing data gathered from a survey of 156 large Italian businesses (249 or more employees). Our study contributes to both theory and practice in information security governance: as for the former, our quantification mechanism (and the underlying approach to data repurposing) can be used by other researchers who face data scarcity around information security (Atapour-Abarghouei *et al.*, 2020); as for the latter, organisational leaders can use our mechanism to determine what their peers consider essential information security governance measures. Finally, our study offers directions for researchers willing to increase the sustainability of their research practices and maximise the efficiency of their research activities, by repurposing an existing data set on information security.

The remainder of the paper is organised as follows: next, we review existing literature on information security governance and formal/informal guidelines and recommendations for practical interventions in information security. The following section describes the methods adopted in our research. We then present the results of our analysis. A discussion of our findings follows, before the conclusion.

2. Literature review

Senior leaders' and board members' commitment is crucial in establishing an effective information security governance system (Damenu and Beaumont, 2017). However, the uplifting of information security "from the basement to the boardroom" (Schinagl and Shahim, 2020) has not been accompanied by the provision of appropriate tools and techniques that board members and other organisational leaders, without an information security background, could use to support their decisions (Mishra, 2015). Information security governance is an under-explored field of study, with the very term "governance" meaning different things to different people (Nicho, 2018). In this review of the literature, we focus on the tension that exists between the need for organisational leaders to make evidence-based information security governance decisions, and the absence of comparison mechanisms to assess adherence to information security governance guidelines.

2.1 Organisational leaders and information security governance

Entrusted with organisational decision-making, top management, executives and BoDs are responsible for, among others, approving or rejecting management initiatives, formulating strategies, overseeing strategy implementation and linking the firm to important external stakeholders (Hoppmann *et al.*, 2019). In recent years, calls for BoDs in particular to take responsibility for information security have been multiplying (Scully, 2014), and so have calls for BoDs to recognise cyber and information security as part of their corporate governance mandate (Von Solms and Von Solms, 2018). After all, BoDs are elected by shareholders to protect their investments.

Significant challenges, however, face organisational leaders in this respect. First, BoDs tend to lack members with skills and knowledge in IT and information security (Aguilar, 2014; PwC, 2012; Valentine and Stewart, 2013). Second, the very disciplines of cyber and information security, characterised by lack of agreed definitions, make the task of non-expert decision-making particularly troublesome, especially at a strategic level (Rothrock *et al.*, 2018; Von Solms and Von Solms, 2018). Third, organisational structures may, at times, confine information security away from the reporting lines of BoDs: research shows that chief information officers (CIOs) rarely report to chief executive officers (CEOs) and are

mostly not board members (Grobman and Cerra, 2016). Fourth, information security investments lack reliable metrics for the BoDs and executives to assess the effectiveness of their efforts in this area (Redseal, 2016). This all leads to a baseline uncertainty reigning in organisations facing the spectre of being hacked and the aligned dilemma of knowing how much to invest in information security (Gordon and Loeb, 2002) and what areas should be covered as a priority (Daniel Schatz and Bashroush, 2018).

Organisational leaders' role in establishing a solid information security governance system is further complicated by the uncertainty that reigns in this domain. Characterised by a mix of practical (the majority) and theoretical (the minority) approaches, the discipline of information security governance is relatively immature, mainly descriptive and with limited empirical or theoretical guidance (Schinagl and Shahim, 2020).

To assist organisational leaders with the "how to" information security governance, several frameworks, models and guidelines have been created. These can be classified as standards, or *standard-like* frameworks/schemes; and guidelines. With respect to *standards*, these are stringent portfolios of "documented, executed, tested, implemented, and monitored controls" (Fitzgerald, 2012, p. 164) aimed at establishing organisational practices that, if followed, should provide guarantees against the loss of confidentiality, integrity and/or availability of data and information. The use of the verb *should* is intentional and captures the closely related problem intrinsic to information security, namely, the difficulty of assessing its performance from both a technical (Agyepong *et al.*, 2020) and a human perspective (Zhang and Ghorbani, 2020). Internationally recognised standards such as ISO27001:2015, national institute of standards and technology (NIST) and control objectives for information and related technologies (COBIT) or regional schemes such as the UK Cyber Essentials and the Australian Essential Eight constitute therefore a generic blueprint for virtuous organisational behaviours, without having the nametag of *laws* and *regulations*. Often, companies can be officially accredited against such standards (e.g. ISO27001:2015, COBIT and Cyber Essentials) or engage in self-assessment for compliance and maturity (e.g. Essential Eight).

Guidelines are sets of recommendations in the form of "how to" lists to help organisations defend themselves against cyber-attacks and are the product of the work of various entities, including public organisations, groups of academics, practitioners, companies, etc. They tend to be less stringent than standards, in that they are less generic and cover specific aspects of cyber and information security, usually not covered by standards, other frameworks and schemes. In this field, scholars and practitioners have been working to provide evidence-based guidelines which can take two formats: conceptual indications and practical measures.

In their first systematic literature review on the topic of information security governance, Schinagl and Shahim (2020) provide a synthetic classification of such frameworks (Table 1).

Overall, frameworks for information security governance suffer from flaws that can be broadly synthesised around the following points (Schinagl and Shahim, 2020): *first*, an information security governance model applicable to all organisations does not exist: industry type, underlying regulatory scenario, years of operations, organisational structure, etc. are all factors that impact the type of model most suitable to a given entity. *Second*, existing frameworks seem to build on a traditional, organisation-centric approach to security governance, one that does not account for the changing threat environment within which modern organisations operate. Longer and more complex supply chains, increasing levels of embeddedness among organisations, changes in the traditional client–supplier relationships, etc. are dynamics that require new forms of governance, also from an information security perspective.

Information security governance models in practice	Information security governance models in research			
	Corporate governance models	Sociotechnical models	Process-oriented models	Cyber-oriented models
Examples				
ISO standards (27001 to 27005)	Posthumus and Von Solms (2004)	Dutta and McCrohan (2002)	Knapp *et al.* (2009)	Kauspadiene *et al.* (2017)
NIST cyberframework	Von Solms and Von Solms (2006)	Veiga and Eloff (2007)	Haufe *et al.* (2016)	Rebollo *et al.* (2015)
COBIT	Park *et al.* (2006)	Maleh *et al.* (2017)	Carcary *et al.* (2016)	Saneei Moghadam and Colomo-Palacios (2018)
ITIL			Nicho (2018)	

Note: ISO: International Standards Organisation

Table 1. Information security governance frameworks

A solution to these limitations is to use more generic sets of guidelines which can be tailored to the needs of the specific organisation. We explore some of these in the next section.

2.2 Guidance on information security governance for Boards of Directors

Among the information security governance guidelines (conceptual or practical), given the complexity of the topic and the cross-functional nature of information security (Ruan, 2019), there is scarcity of specific directions and recommendations for organisational leaders. Various explanations exist for such paucity. *First*, in spite of undeniable advancements in this field, a traditional *technical-first* approach to information security is still widespread (Soomro *et al.*, 2016). This translates in the relegation of information security to a mere operational issue, for which strategic considerations are secondary. *Second*, and associated to the previous point, efforts to shape an information security leadership in organisations are a relatively new requirement. An example of this is the recent acknowledgement by BoDs of the importance of managing cyber risks effectively. In an address to the New York Stock Exchange in 2014, Commissioner Luis A. Aguilar of the US Securities and Exchange Commission noted: "[. . .] evidence suggests that there may be a gap that exists between the magnitude of the exposure presented by cyber-risks and the steps, or lack thereof, that many corporate boards have taken to address these risks [. . .]" (2014). Third, more simply, organisations whose core business is not information security may not yet see the need to invest in this area at a leadership level.

Among the research offering practical recommendations for interventions in information security governance by top management, executives and BoDs, two papers stand out for the practical approach they adopt, and the comprehensiveness of the guidance offered. Zukis (2016) and Renaud *et al.* (2019) discuss a series of practical recommendations extracted from existing literature and offer an exhaustive list of practical interventions for enhanced information security governance. Table 2 proposes a synthesis of the recommended interventions around ten main areas.

The effectiveness of evidence-based frameworks similar to the ones proposed by Zukis (2016) and Renaud *et al.* (2019) is directly associated with the need to understand whether, and how, modern organisations, knowingly or unknowingly, implement them. Information management and information security governance are rich, transversal disciplines within

Action/recommendation area	Zukis (2016)	Renaud *et al.* (2019)
Organisational structure and governance	Creating a separate board-level IT committee	Have a cyber expert in the BoD
	Adding a director with IT and cybersecurity skills to the board	Have a BoD committee overseeing CS
	Modifying the reporting structure of the CISO (chief information security officers) from the CIO to another executive, including the CEO	Committee should report to the BoD on a regular basis
Organisational culture	Viewing IT governance and cyber risk as a business issue that spans people, process and technology	Monitor cyber-culture
	Ensuring that employees are regularly educated around emerging and ongoing risks and mitigation practices	Regular awareness training
Risk management and frameworks	Regularly reviewing, at the board level, IT governance and cybersecurity risk from a strategy, policy and active-threat perspective	Act to proactively detect intrusions (security) and mistakes (safety)
	Requiring and reviewing the results of regular proactive threat and vulnerability assessments	Monitoring of new cyber/physical risks, including knowledge risks
	Identifying and aligning risk with critical parts of a business and ecosystem	Select best cybersecurity mechanisms and associated standards (e.g. NIST)
	Integrating IT governance and cyber risk into an overall enterprise risk approach	
	Adopting and applying a structured IT governance and cyber risk framework	
Budget and insurance	Reviewing IT security budgets and the policies and procedures in place to prevent, protect, detect and respond to IT governance or cybersecurity issues	Balanced and sustained cybersecurity spending
	Periodically reviewing levels of cyber risk insurance and coverage	Take out cyber insurance
Cyber response	Having a crisis response approach in place and reviewing it regularly	Adopt a breach management plan Appoint a rapid response team
Strategies and action plans	As this issue continues to evolve, monitoring and adopting leading practices is also a vital practice to manage ongoing risks and vulnerabilities	Formulate plans of actions and refresh them annually Oversee plans of action, with appointment of key account manager Adopt a business continuity plan
Supply chain management	Engaging third-party business partners in a holistic assessment of risk and mitigating options across an ecosystem	Retain/hire consultants to assess cyber-governance mechanisms Retain/hire lawyers for legal implications Retain/hire expert company in cyber-response Ensure stakeholder security practice

Table 2. Practical recommendations for organisational leaders [from Zukis (2016) and Renaud *et al.* (2019)]

(*continued*)

Action/recommendation area	Zukis (2016)	Renaud *et al.* (2019)
		Assess cybersecurity measures of SHS/vendors
		Ensure contractors treat IC-information confidentially/securely
		Retain/hire cyber talent
		Invest in ethical hacking
Asset management	Ensuring management assesses and understands relative information asset risk across the business	Identify tangible and intangible organisational assets
		Prioritise such assets for risk management purposes
Information sharing	Ensuring that company leadership supports the active participation in industry and public efforts to create standards and share information and leading practices	Organise organisational learning sessions post-emergency
Others		Improve measures for the security of internet-related knowledge

Table 2.

which different interventions can contribute to the achievement of objectives. Implementation of such measures goes a long way towards enhancing business resilience: preventing information security incidents as much as possible, and then responding to incidents that *do* occur. Even so, established mechanisms to assess adherence to sets of guidelines, especially when there is no direct mapping from the gathered data to the guidelines, are lacking. The present research seeks to address this gap.

2.3 Conceptual framework and research questions

The present study proposes an interpretive framework to quantify the extent to which data can be repurposed to gauge implementation of information security governance guidelines aimed at top management, executives and BoDs. Given its completeness and practical focus, we selected the framework proposed by Renaud *et al.* (2019) and quantified the extent to which their guidelines are being followed. Answering this question can offer important insights into the gaps that exist between the *theory* of information security governance in terms of recommended practical measures and best practice, and *the actual practice* of companies in the field.

It is indeed possible that the available data does not contain questions which map to each construct. In these cases, we satisfice, quantifying what we *do* have data for, and ensuring that when the results are reported, it is made clear which parts of the framework were measured.

The contribution of our study resides in the mechanism for deriving a quantitative adherence assessment, which supports inter-organisational comparisons by all stakeholders. The research questions being addressed are aligned with the challenges identified by Ruan (2019):

RQ1. How can we quantify implementation of information security governance guidelines using repurposed survey data?

RQ2. How can we support companies in gauging how well they are following a specific set of information security governance recommendations, as compared to other organisations of similar size and industry?

The next section outlines the methods we adopted for this study.

3. Research methodology

In our study, we formulated a quantification mechanism, which is composed of the following steps (Figure 1).

3.1 Step 1: mapping

Two information security experts discussed each variable, and independently identified which variables could be mapped to each category in the set of guidelines proposed by Renaud *et al.* (2019). They then discussed discrepancies and differences, until an agreed-upon assessment framework was identified. To further test the validity of the resulting assessment framework, relevant literature was consulted, to confirm or reject the proposed attributions. In cases in which no existing literature confirmed the proposed mapping, the two experts reviewed their mappings. The process was repeated until agreement between the two experts was reached. For example, for the "Select best cybersecurity mechanisms and associated standards" recommendation from Renaud *et al.* (2019), the mapped variables from the survey are presented in Table 3. As shown, 11 variables in the survey were allocated to this category (responding to three questions in the survey) and elicited responses from the participant on their involvement in various cybersecurity-related duties and the organisational investment in, and appetite for, four specific job positions. The column "Possible responses" lists the answers that each participant could give to the related questions and the column "Explanation for the attribution" illustrates the rationale for mapping. Finally, the column "Supporting literature" indicates sources that confirm the validity of the attribution. It is essential to note that the validity of our attribution is further strengthened by the usage of multiple variables for most of the recommendations provided in the adopted framework (Renaud *et al.*, 2019).

Appendix contains the complete survey instrument, with an overview of the categories within the framework, the variables mapped to each category and their total number and the literature in support of the attribution. Besides literature support, we acknowledge the possible limitations of our mapping, as the recommendations provided in the adopted framework are mostly composed by a portfolio of possible actions taken by organisations (e.g. a mix of people, processes and policies could influence their implementation). The survey variables used to measure adherence to the recommendations are, at best, proxies. To overcome this, we offer a point-by-point explanation of the rationale used for our mapping, equally contained in Appendix (column: Mapping rationale).

3.2 Step 2: data cleaning and preparation

Step 2a) Qualitative measures were converted to quantitative ones for statistical analysis. As an illustration, answers that could be attributed to a five-point Likert scale (from

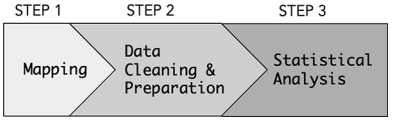

Figure 1.
Adopted methodology

Table 3. Example of variables ascribed to one of the recommendations in the framework

Recommendation category (Renaud *et al.*, 2019)	Variables	Possible responses (from the survey)	Explanation for the attribution	Supporting literature
Select best cybersecurity mechanisms and associated standards	Question (from the survey): *What is the CISO's involvement with each of the following activities?*			
	Definition of security architecture Scouting of security products Policy and security framework definition	Someone else in charge; Occasionally involved; Responsible	The CISO's involvement with the three listed activities indicates how cybersecurity leadership in the organisation engages in the selection of the best cybersecurity mechanisms and associated standards	Chang and Hawamdeh (2020) Tselios *et al.* (2020) Von Solms and Von Solms (2008)
	Question (from the survey): *Does your company have individuals in the following job positions?*			
	Security administrator Security analyst Security architect Security engineer	Yes; No	The presence of these professional figures in the organisation contributes to organisational efforts in identifying best practices in cybersecurity mechanisms and associated standards	Allen *et al.* (2015) Allen *et al.* (2015) Allen *et al.* (2015) Allen *et al.* (2015)
	Total variables included in the mapping: 7			

Strongly disagree to Strongly agree) were converted to quantitative values ranging from 1 to 5, respectively. For example, if a respondent had selected "disagree" to a specific question, this response would then be converted into a quantitative measure or score of 2/5 or 0.4 (we refer to the converted measure as the "score" in subsequent discussions).

Step 2b) Categories of guidelines were excluded for which we could not find corresponding variables. We also excluded variables which reported high missing proportions (i.e. >20%). The exclusion of variables with high missing rates did not necessarily result in a loss of interpretation of the various categories, as the main qualitative questions in the survey could still be mapped to categories in the framework. Multiple variables were ascribed to the categories, which compensated for the excluded variables because of missing proportions and allowed us to calculate the related score (Appendix).

Step 2c) Based on the number of variables attributed to a category, after variable exclusion, the maximum possible score for a category could be determined. This maximum possible score value was used in calculation of the quantitative measure.

Step 2d) Scores were calculated for each of the framework categories. The score value can be interpreted as the adherence to the evidence-based recommendations offered in Renaud *et al.* (2019). The range of the scores are in the interval 0–1, where a value closer to 0 would indicate poor/low adherence to the recommendation and values closer to 1 would indicate strong/high adherence to the recommendations in Renaud *et al.* (2019).

3.3 Step 3: statistical analysis

We calculated descriptive statistics to illustrate adherence to the framework's categories. We used this methodology to analyse a database of 156 Italian large corporations (249 employees or plus). The database originated from a survey conducted by a public university in Italy in 2017. Purpose was to assess what privacy and information security systems and governance models such organisations were executing, considering the entry into force of the General Data Protection Regulations (GDPR) in Europe. Respondents were professionals responsible for cyber and information security (CISOs, CSOs), IT Directors and CIOs and personnel in charge of compliance. Each response reflected the practices of a single organisation, for a total of 156 in the following industries: Manufacturing, Services, Retail, Utility and Energy, Public Administration and Healthcare, Finance (including banking and insurance), Telecommunications and Media and Other. The survey, administered in Italian, was composed of quantitative and qualitative questions, open-ended or multiple-choice.

4. Results

Based on the initial analysis of the scored responses, there was an overall average level of adherence (0.620) to the guidelines proposed by Renaud *et al.* (2019) (Table 4). The overall average level was calculated by an aggregation of the category scores using equal weighting.

Figure 2 illustrates that a normal distribution could be observed for the overall average scores across our sample, with a slight tail to the left. Interestingly, there were no observations reporting overall average score values in the 0.900–1.000 range (i.e. a high level of adherence to the selected framework of recommendations).

Table 4. Overall average adherence score

No. of observations	Average	Min	Max	Lower 95%	Upper 95%
156	0.620	0.270	0.851	0.600	0.641

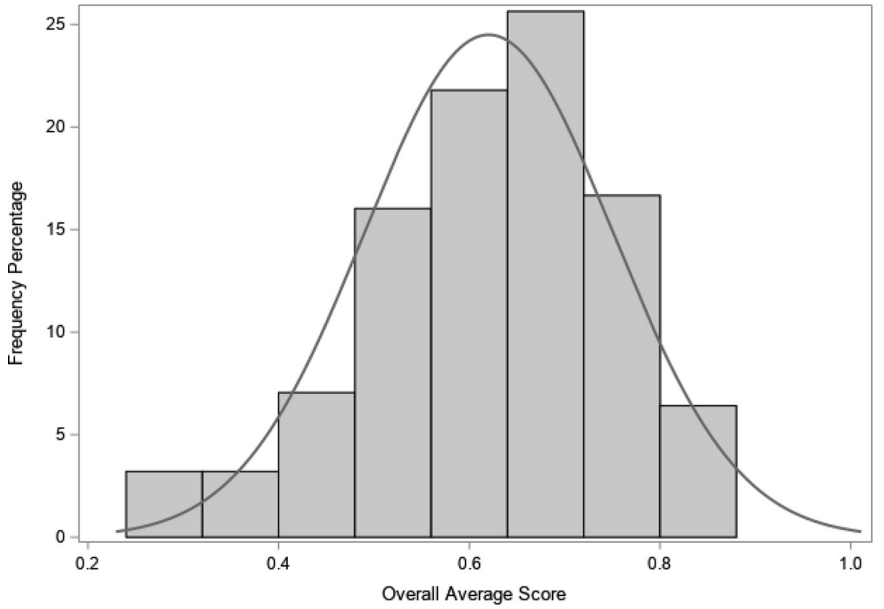

Figure 2. Distribution of adherence scores across the sample ($n = 156$)

Industry	No. of observations	Average	Min	Max	Lower 95% CI	Upper 95% CI
Finance (banks – insurances)	27	0.652	0.270	0.831	0.594	0.710
Manufacturing	45	0.627	0.337	0.849	0.592	0.662
Other	25	0.599	0.372	0.851	0.546	0.652
Public sector and health	10	0.595	0.270	0.801	0.457	0.732
Retail and large-scale retail	20	0.567	0.332	0.763	0.511	0.623
Service	8	0.655	0.544	0.803	0.579	0.731
Telecommunications and media	8	0.577	0.285	0.783	0.445	0.709
Utility and energy	12	0.680	0.528	0.846	0.629	0.732

Table 5. Average and 95% confidence interval (CI) adherence score per industry

An analysis of the scores per industry (Table 5) was carried out by taking the adherence score value of each category for each participant and aggregating them based on the reported industry of the participating organisation.

Finance reported higher adherence to the framework, based on the average and confidence interval bounds. Although some industries reported slightly higher average score values (e.g. Service and Utility and Energy), these industries also had a smaller number of observations (e.g. <20). The Retail and Large-Scale Retail industry accounted for the lowest average score value. Overall, all industries reported an average score value above 0.560, with no industry reporting an average score greater than 0.700. Some industries were found to have outliers above the 1.5× inter-quartile range and with score values above 0.800 (with 1 been a perfect score). Dispersion in the Finance industry was at a higher average score value as compared to the other industries (Figure 3). We also found that this industry contained two outliers below the 1.5× inter-quartile range.

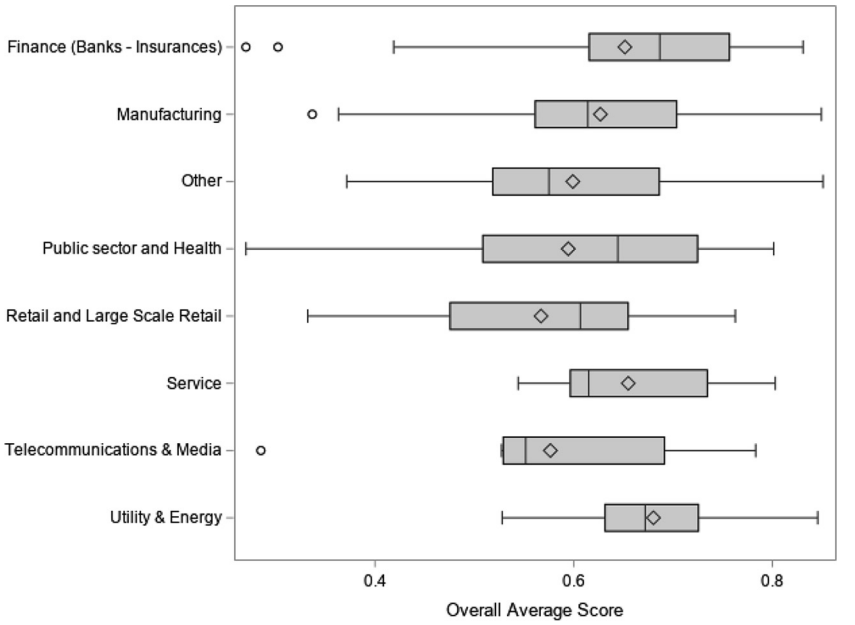

Figure 3.
Overall average adherence score per industry

Notes: *The average in each respective boxplot is indicated by the diamond symbol and the median by the line inside the box

Our analysis extended to include the adherence score for each recommendation in the adopted framework (Table 5). The "Cybersecurity mechanisms and standards" category, referring to the recommendation for organisations to invest in identifying the best information security mechanisms, scored the highest average value. The confidence interval was at a 0.701–0.759 range compared to other categories, showing an expected higher level of adherence amongst participants.

Interestingly, along with this category, another two recommendations ("Intangible/tangible assets", i.e. organisations' investments in mapping such assets; and the associated "Prioritisation of assets for risk management purposes") reported an average adherence score value above 0.700. With regard to the maximum average score values, there were observations in certain categories which reported a perfect score value (i.e. perfect adherence). However, this does need to be weighed against the average score value for the category and hence the confidence intervals given in Table 6 would be a better reflection of the adherence level. A more detailed discussion of the results is given in the next section.

5. Discussion

Our approach assesses adherence to evidence-based information security governance guidelines by public and private sector organisations, based on our mechanism for repurposing existing survey data. To test our approach, we used a survey on information security and privacy to quantify organisational adherence to an evidence-based framework (Renaud *et al.*, 2019). Translating the qualitative and quantitative answers from the survey into numerical scores allowed us to answer our RQ1 and RQ2.

Recommendation category	No. of observations	Average	Min	Max	Lower 95%	Upper 95%
CS mechanisms and standards	156	0.730	0.235	1	0.701	0.759
Intangible/tangible assets	148	0.720	0.143	1	0.685	0.755
Prioritising of assets for risk management purposes	148	0.720	0.143	1	0.685	0.755
Rapid response team	150	0.680	0.167	1	0.642	0.718
Monitoring of risks	156	0.675	0.053	0.947	0.639	0.711
Acquisition/retainment cyber talent	156	0.671	0.500	1	0.645	0.696
Investment in ethical hacking	156	0.641	0.500	1	0.605	0.677
Breach management plan	156	0.603	0.500	1	0.582	0.623
Committee should report to the BoD on a regular basis	155	0.557	0.077	0.885	0.530	0.584
Proactive security and safety measures	156	0.511	0.026	0.816	0.487	0.536
Monitor cyber-culture	153	0.504	0.030	0.788	0.482	0.527
Improvement of measures	151	0.495	0.061	0.788	0.472	0.519

Table 6.
Overall average score by recommendation category

Given the lack of similar approaches in the literature, one way to assess the efficacy of our method is to compare our findings with literature on compliance to information security governance recommendations. Our results confirm that the Finance industry has a higher adherence level to the proposed framework as compared to other industries, based on average (0.652) and confidence interval bounds. Besides being a highly regulated industry, Finance is commonly described as an industry that spends top dollars in cybersecurity (Cyriac and Sadath, 2019).

Other industries also demonstrated high adherence to the framework. Manufacturing and Utility and Energy (Figure 3) contained outlier observations above the 1.5× inter-quartile range (i.e. high adherence to the proposed framework). Overall, all industries showed average adherence levels to the proposed framework with none having an average score value above 0.700. Consistently with literature (Ki-Aries and Faily, 2017), this result highlights how, in spite of the broad portfolio of information security interventions available for modern companies across the people, process and technology triad, there remains significant work to be done (Ruan, 2019).

The results of our analysis on the recommendation categories in the adopted framework that registered the highest levels of adherence in our sample are particularly relevant. Three such categories are worth mentioning, namely, "Select the best cybersecurity mechanisms and associated standards", and the closely related "Intangible/tangible assets" and "Prioritisation of assets for risk management purposes". Here, too, our findings align with the literature. Information security experts agree on the need for modern organisations to apply, in the first place, standardised solutions and practices in information security governance (Jennex and Zyngier, 2007), being that in the field of smart grids (Leszczyna, 2018), cyber-risk management (Collier *et al.*, 2014) or cyber-response (Nespoli *et al.*, 2018). Posthumus and Von Solms (2004) argue that organisational information assets are subject to two types of cyber-risks, external and internal to the organisation itself. Incorporated in the provisions of risk management standards such as ISO31000 and ISO27001, the identification of cyber-risks requires a preliminary step, the recognition of tangible and intangible assets (Bongiovanni *et al.*, 2020).

Mapping and prioritising the most fundamental organisational assets for cyber-risk management purposes is therefore an acknowledged imperative in information security governance practice and research (Roldán-Molina *et al.*, 2017), especially considering contextual factors such as resource scarcity, increased digital footprint (Aliyu *et al.*, 2020) and diffusion of well-established risk management standards.

A discussion of the recommendation categories that, on the contrary, registered low adherence by the organisations can offer further insights on the type of interventions organisational leaders prioritise. "Proactive security and safety measures" registered the third lowest level of adherence (0.511), a finding that can be explained by the acknowledged challenge that modern organisations have in steering away from a reactive approach to information security to endorse a more proactive stance, where cyber-risks are anticipated, and not responded to Graves (2019).

"Monitoring of cyber-culture" is the recommendation that scored the second lowest level of adherence (0.504), denoting that organisations in our sample prioritised investments in other areas. Besides the challenges associated with the definition of information security culture, there is an acknowledged difficulty by organisations to select the appropriate mix of management practices and initiatives to build a solid information security culture (Alshaikh, 2020).

The recommendation that scored the lowest adherence score (0.495) was "Improve measures for the security of internet-related knowledge". Framing information security from the perspective of knowledge is a relatively recent exercise, one that requires further efforts (Ilvonen, 2013). To explain the relatively low score of this recommendation in our sample, we can hypothesise that organisational leaders have not fully grasped this *knowledge-centric* approach.

5.1 Theoretical and practical contributions

The present research offers a novel methodology to measure how organisations adhere to a set of evidence-based recommendations aimed at organisational leaders in information security governance. From a theoretical perspective, our proposed methodology addresses an acknowledged gap in the information security literature, namely, the lack of instruments to assess organisational investments (Moore *et al.*, 2015; Ruan, 2019). Our approach offers a way to assess the degree of adherence to selected recommendations, by repurposing the answers in a survey into a global adherence score. Moreover, our approach aligns with calls in the literature on sustainable research practices that recommend scholars to avoid wasted resources and consider, where possible, re-using existing data sets and methods to address similar research questions (Ligozat *et al.*, 2020).

From a practical perspective, the proposed approach gives organisational leaders in information security (e.g. CISOs, CIOs, Board members, etc.) a chance to have a holistic view on their investments by means of comparison. Our approach also addresses the acknowledged issue of "survey fatigue", which particularly affects cybersecurity (Clair and Girard, 2020). The collection of primary data should be the preferential approach. This is nonetheless not always possible, and economical. Further, cybersecurity professionals are regularly asked to complete surveys by consulting companies and scholars. Resulting fatigue can lead to loss of data quality. We see in the repurposing of existing survey data an efficient (and effective) method to have a better understanding of how an organisation performs in this field.

Finally, our approach has the potential to address the so-called "cybersecurity data sharing paradox" (Atapour-Abarghouei *et al.*, 2020) by which public and private interests clash when it comes to sharing data to combat cyber-crime. By effectively repurposing existing survey data, we reduce the number of "data requests" to organisations, a significant move in a context of data scarcity and resistance to sharing.

5.2 Research limitations and areas for future research

Our research retrospectively measured how organisations fared in terms of adherence to the information security governance recommendations proposed by Renaud *et al.* (2019), using

repurposed data from a previous survey. Had the framework been published prior to the survey, with sufficient dissemination, the results of our study could have been different. The justification for the adopted approach stems from the scarcity of information security literature proposing holistic guidelines for companies to *be better* in information security governance. In particular, what is missing in the literature is an operationalisation of existing recommendations, one that associates guidelines with methods for executing and measuring them (Goss, 2017). By assessing surveyed organisations' adherence to a later framework, we aimed at establishing one such method, and an approach that can be easily replicated in future studies and executed in practice. We acknowledge that our mapping mechanism could be perceived as imperfect: other information security experts could suggest a different mix of variables to measure adherence to the recommendations contained in the investigated information security governance framework (Renaud *et al.*, 2019). Nonetheless, two elements make our approach valid nonetheless: first, organisations willing to use our method to benchmark themselves against competitors or other companies would need to agree on the variables used to measure adherence to the selected recommendations; second, our approach is a starting point, for which we invite other researchers to join us in improving.

One final limitation in our study is the fact that the literature review we conducted to ensure the validity of our attribution of governance recommendations in the selected framework to variables in the survey was not systematic, and some information sources could have been missed. Again, we invite other researchers to join us in performing a comprehensive assessment of current literature, to create further opportunities for repurposing survey data to assess existing information security governance frameworks.

6. Conclusion

In this study, we proposed and tested a mechanism for repurposing existing survey data to assess organisations' adherence to a framework of information security governance guidelines on 156 large Italian organisations. The main contribution of our work is the quantification methodology for repurposing data, which facilitates peer comparison, and can push organisations to improve their security practices. Our analysis confirms findings in existing literature related to the kinds of industries which are more responsive to information security best practices and highlights the interventions that are most often deployed by such organisations. Furthermore, through its repurposing of an existing data set, our approach aligns with calls in the literature for more efficient and sustainable research practices.

References

Abawajy, J. (2014), "User preference of cyber security awareness delivery methods", *Behaviour and Information Technology*, Vol. 33 No. 3, pp. 237-248.

Abu-Amara, F., Almansoori, R., Alharbi, S., Alharbi, M. and Alshehhi, A. (2021), "A novel SETA-based gamification framework to raise cybersecurity awareness", *International Journal of Information Technology*, Vol. 13 No. 6.

Aguilar, L.A. (2014), "Boards of directors, corporate governance and cyber-risks: sharpening the focus", *Cyber Risks and the Boardroom Conference*, New York, NY Stock Exchange, New York, NY.

Agyepong, E., Cherdantseva, Y., Reinecke, P. and Burnap, P. (2020), "Challenges and performance metrics for security operations center analysts: a systematic review", *Journal of Cyber Security Technology*, Vol. 4 No. 3, pp. 125-152.

Aliyu, A., He, Y., Yevseyeva, I. and Luo, C. (2020), "Cyber security decision making informed by cyber threat intelligence (CYDETI): IEEE CNS 20 poster", Paper presented at the 2020 IEEE Conference on Communications and Network Security (CNS).

Allen, J.H. Crabb, G. Curtis, P.D. Fitzpatrick, B. Mehravari, N. and Tobar, D. (2015), "Structuring the chief information security officer organization", Retrieved from.

Alshaikh, M. (2020), "Developing cybersecurity culture to influence employee behavior: a practice perspective", *Computers and Security*, Vol. 98, p. 102003.

Atapour-Abarghouei, A. McGough, A.S. and Wall, D.S. (2020), "Resolving the cybersecurity data sharing paradox to scale up cybersecurity via a co-production approach towards data sharing".

Bair, J., Bellovin, S.M., Manley, A., Reid, B. and Shostack, A. (2017), "That was close: reward reporting of cybersecurity near misses", *Colo. Tech. LJ*, Vol. 16, p. 327.

Barlette, Y., Gundolf, K. and Jaouen, A. (2017), "CEOs' information security behavior in SMEs: does ownership matter?", *Systèmes D'information and Management*, Vol. 22 No. 3, pp. 7-45.

Bilal, K. (2011), "Effectiveness of information security awareness methods based on psychological theories", *African Journal of Business Management*, Vol. 5 No. 26, doi: 10.5897/AJBM11.067.

Bongiovanni, I., Renaud, K. and Cairns, G. (2020), "Securing intellectual capital: an exploratory study in Australian universities", *Journal of Intellectual Capital*, Vol. 21 No. 3, pp. 481-505.

Briggs, P., Jeske, D. and Coventry, L. (2017), *Human Aspects of Information Security, Privacy and Trust*, Vol. 10292, Springer International Publishing, Cham, pp. 3-13.

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.

Chang, H.-C. and Hawamdeh, S. (2020), *Cybersecurity for Information Professionals*, CRC Press, Milton.

Chen, X., Susilo, W. and Bertino, E. (2021), *Cyber Security Meets Machine Learning*, Springer, Singapore.

Clair, N.S. and Girard, J. (2020), "Are cybersecurity professionals satisfied with recent cybersecurity graduates?", *Journal of the Colloquium for Information Systems Security Education*, Vol. 7 No. 1, pp. 7-7.

Collier, Z.A., DiMase, D., Walters, S., Tehranipoor, M.M., Lambert, J.H. and Linkov, I. (2014), "Cybersecurity standards: managing risk and creating resilience", *Computer*, Vol. 47 No. 9, pp. 70-76.

Corradini, I. (2020), "Training methods", *Building a Cybersecurity Culture in Organizations: How to Bridge the Gap between People and Digital Technology*, Springer International Publishing, Cham, pp. 115-133.

Cyriac, N.T. and Sadath, L. (2019), "Is cyber security enough-a study on big data security breaches in financial institutions", Paper presented at the 4th International Conference on Information Systems and Computer Networks (ISCON), Mathura, 21-22 November.

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.

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.

Esparza, J., Caporusso, N. and Walters, A. (2020), *Advances in Human Factors in Cybersecurity*, Vol. 1219, Springer International Publishing, Cham, pp. 88-94.

Fitzgerald, T. (2012), *Information Security Governance Simplified from the Boardroom to the Keyboard*, 1st ed., CRC Press, Boca Raton, FL.

Gordon, L.A. and Loeb, M.P. (2002), "Return on information security investments: myths vs. realities", *Strategic Finance*, Vol. 84 No. 5, p. 26.

Gordon, W.J., Wright, A., Glynn, R.J., Kadakia, J., Mazzone, C., Leinbach, E. and Landman, A. (2019), "Evaluation of a mandatory phishing training program for high-risk employees at a US

healthcare system", *Journal of the American Medical Informatics Association*, Vol. 26 No. 6, pp. 547-552.

Goss, D.D. (2017), "Operationalizing cybersecurity – framing efforts to secure US information systems", *The Cyber Defense Review*, Vol. 2 No. 2, pp. 91-110.

Graves, J. (2019), "Reactive vs. proactive cybersecurity: 5 reasons why traditional security no longer works", available at: www.fortinet.com/blog/industry-trends/reactive-vs–proactive-cyber security–5-reasons-why-traditional

Grobman, S. and Cerra, A. (2016), *The Second Economy: The Race for Trust, Treasure and Time in the Cybersecurity War*, Apress, Berkeley, CA.

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.

He, W. and Zhang, Z. (2019), "Enterprise cybersecurity training and awareness programs: recommendations for success", *Journal of Organizational Computing and Electronic Commerce*, Vol. 29 No. 4, pp. 249-257.

Hoppmann, J., Naegele, F. and Girod, B. (2019), "Boards as a source of inertia: examining the internal challenges and dynamics of boards of directors in times of environmental discontinuities", *Academy of Management Journal*, Vol. 62 No. 2, pp. 437-468.

Ilvonen, I. (2013), "Knowledge security-a conceptual analysis", Tampere University, Tampere, Finland, available at: https://trepo.tuni.fi/handle/10024/114659

Institute of Directors New Zealand (2018), "Reporting cybersecurity to boards", available at: https://f.hubspotusercontent40.net/hubfs/2631546/IoD-Reporting-cybersecurity-to-boards.pdf

IT Governance Institute (2006), *Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2nd ed., IT Governance Institute, Rolling Meadows, IL.

IT Governance Privacy Team (2020), *EU General Data Protection Regulation (GDPR) – an Implementation and Compliance Guide*, 4th ed., IT Governance Publishing.

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

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.

Khan, F., Kim, J.H., Mathiassen, L. and Moore, R. (2021), "Data breach management: an integrated risk model", *Information and Management*, Vol. 58 No. 1, p. 103392.

Ki-Aries, D. and Faily, S. (2017), "Persona-centred information security awareness", *Computers and Security*, Vol. 70, pp. 663-674.

Klein, A., Manini, R. and Shi, Y. (2020), "Across the pond: how U.S. Firms' boards of directors adapted to the passage of the GDPR", *SSRN*, doi: 10.2139/ssrn.3640515.

Knapp, K.J., Franklin Morris, R., 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.

Le Blanc, K. and Freeman, S. (2016), *Advances in Human Factors in Cybersecurity*, Vol. 501, Springer International Publishing, Cham, pp. 223-228.

Leszczyna, R. (2018), "A review of standards with cybersecurity requirements for smart grid", *Computers and Security*, Vol. 77, pp. 262-276.

Ligozat, A.-L., Neveol, A., Daly, B. and Frenoux, E. (2020), "Ten simple rules to make your research more sustainable", *PLoS Computational Biology*, Vol. 16 No. 9.

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 Security*, Vol. 12 No. 6.

Merrick, R. and Ryan, S. (2019), "DATA PRIVACY GOVERNANCE IN the AGE OF GDPR: a surge of new data protection regulations is forcing Canadian and U.S. companies to reassess how they process and safeguard personal information", *Risk Management*, Vol. 66 No. 3, p. 38.

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

Moore, T. Dynes, S. and Chang, F. (2015), "Identifying how firms manage cybersecurity investment", 32, available at: https://cpb-us-w2.wpmucdn.com/blog.smu.edu/dist/e/97/files/2015/10/SMU-IBM.pdf

Nespoli, P., Papamartzivanos, D., Gomez Marmol, F. and Kambourakis, G. (2018), "Optimal countermeasures selection against cyber attacks: a comprehensive survey on reaction frameworks", *IEEE Communications Surveys and Tutorials*, Vol. 20 No. 2, pp. 1361-1396.

Nicho, M. (2018), "A process model for implementing information systems security governance", *Information and Computer Security*, Vol. 26 No. 1, pp. 10-38.

Nolan, R. and McFarlan, F.W. (2005), "Information technology and the board of directors", *Harvard Business Review*, Vol. 83 No. 10, pp. 96-157.

Park, H., Kim, S. and Lee, H.J. (2006), "General drawing of the integrated framework for security governance", Paper presented at the Knowledge-Based Intelligent Information and Engineering Systems, Berlin, Heidelberg.

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.

PwC (2012), *Bridging the IT Confidence Gap (Abridged Version)*, Retrieved from New York, NY.

Rebollo, O., Mellado, D. and Fernandez-Medina, E. (2015), "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. (2015), "Empirical evaluation of a cloud computing information security governance framework", *Information and Software Technology*, Vol. 58, pp. 44-57.

Redmiles, E.M., Warford, N., Jayanti, A., Koneru, A., Kross, S., Morales, M., Stevens, R. and Mazurek, M. L. (2020), "A comprehensive quality evaluation of security and privacy advice on the web", Paper presented at the 29th USENIX Security Symposium (USENIX Security 20), Boston, MA, 12-14 August.

Redseal (2016), "The rise of cyber-overconfidence in C-Suite", available at: www.redseal.net/wp-content/uploads/2016/12/RedSeal-CEO-Survey-Executive-Summary.pdf

Refsdal, A., Solhaug, B. and Stølen, K. (2015), *Cyber-Risk Management*, 1st ed., 2015. ed., Springer International Publishing: Imprint: Springer, Cham.

Renaud, K., Von Solms, B. and Von Solms, R. (2019), "How does intellectual capital align with cyber security?", *Journal of Intellectual Capital*, Vol. 20 No. 5, pp. 621-641.

Roldán-Molina, G., Almache-Cueva, M., Silva-Rabadão, C., Yevseyeva, I. and Basto-Fernandes, V. (2017), "A comparison of cybersecurity risk analysis tools", *Procedia Computer Science*, Vol. 121, pp. 568-575.

Rothrock, R.A., Kaplan, J. and Van Der Oord, F. (2018), "The board's role in managing cybersecurity risks", *MIT Sloan Management Review*, Vol. 59 No. 2, pp. 12-15.

Ruan, K. (2019), *Digital Asset Valuation and Cyber Risk Measurement: principles of Cybernomics*, Academic Press, London.

Saneei Moghadam, R. and Colomo-Palacios, R. (2018), "Information security governance in big data environments: a systematic mapping", doi: 10.1016/j.procs.2018.10.057.

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.

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

Schinagl, S. and Shahim, A. (2020), "What do we know about information security governance?: 'from the basement to the boardroom': towards digital security governance", *Information and Computer Security*, Vol. 28 No. 2, pp. 261-292.

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

Sheng, Q.-W. (2020), *e-Learning, e-Education, and Online Training*, Vol. 340, Springer International Publishing, Cham, pp. 25-37.

Siponen, M.T. (2001), "Five dimensions of information security awareness", *Computers and Society*, Vol. 31 No. 2, pp. 24-29, doi: 10.1145/503345.503348.

Sobers, R. (2021), "134 cyber security statistics and trends for 2021", available at: www.varonis.com/blog/cybersecurity-statistics/

Soomro, Z., Shah, M. 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.

Teplinsky, M. (2013), "Fiddling on the roof: Recent developments in cybersecurity", *American University Business Law Review*, Vol. 2 No. 2, pp. 225.

Trim, P. and Upton, D. (2013), *Cyber Security Culture*, Routledge, Farnham.

Tselios, C., Tsolis, G. and Athanatos, M. (2020), *Computer Security*, Vol. 11981, Springer International Publishing, Cham, pp. 3-18.

UK Government (2020), "Cyber security breaches survey 2020", available at: www.gov.uk/government/statistics/cyber-security-breaches-survey-2020

Valentine, E.L.H. and Stewart, G. (2013), "The emerging role of the board of directors in enterprise business technology governance", *International Journal of Disclosure and Governance*, Vol. 10 No. 4, pp. 346-362.

Van Steen, T. and Deeleman, J. (2021), "Successful gamification of cybersecurity training", *Cyberpsychology, Behavior and Social Networking*, Vol. 24 No. 9, pp. 593-598.

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

Von Solms, B. (2006), "Information security – the fourth wave", *Computers and Security*, Vol. 25 No. 3, pp. 165-168.

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.

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

Von Solms, S. and Von Solms, R. (2008), *Information Security Governance*, Springer Science and Business Media.

Williams, E.J., Hinds, J. and Joinson, A.N. (2018), "Exploring susceptibility to phishing in the workplace", *International Journal of Human-Computer Studies*, Vol. 120, pp. 1-13.

Wylie, P.L. and Crawley, K. (2021), *The Pentester Blueprint: starting a Career as an Ethical Hacker*, John Wiley, Indianapolis, IN.

Zhang, X. and Ghorbani, A. (2020), "Human factors in cybersecurity: issues and challenges in big data", *Security, Privacy, Forensics Issues in Big Data*, pp. 66-96.

Zukis, B. (2016), "Information technology and cyber security governance in a digital world", in Leblanc, R. (Ed.), *The Handbook of Board Governance*, John Wiley and Sons, Inc, Hoboken, NJ, pp. 555-573.

Appendix. Variable attribution

Action/ recommendation area	Recommendation category (Renaud *et al.*, 2019)	Variables (mapped from the survey)	Possible responses (from the survey)	Mapping rationale (and main focus: people, processes and policies)	Supporting literature
Organisational structure and governance	Have a cyber expert in the BoD	Insufficient survey responses			
	Have a BoD committee overseeing CS	Insufficient survey responses			
	Committee should report to the BoD on a regular basis	FTE with Information Security duties?	Number (continuous)	Having a larger number of professionals dedicated to information security helps addressing the disconnect between BoDs and IT departments, and expands the opportunities for BoDs to be better informed about organisational requirements in the field (people)	Von Solms (2006)
		Infosec: Investment trend in the next 12 months?	Decrease; Stable; Increase	Growing information security investments can signal that an organisation has a strategic view on this matter (people, processes and policies)	Nolan and McFarlan (2005)
		FTE with Privacy duties?	Number (continuous)	Having a larger number of professionals dedicated to privacy expands the opportunities for BoDs to be better informed about organisational requirements in the field (people)	Merrick and Ryan (2019)
		Privacy: Investment trend in the next 12 months?	Decrease; Stable; Increase	Growing privacy investments can signal that an organisation has a strategic view on this matter (people, processes and policies)	Klein *et al.* (2020)
		Investment plan for information security and privacy? To what extent?	No, budgeting occurs on a contingency basis; Yes, an annual one; Yes, a multi-year one; Yes, a multi-year one included in the strategic plan	BoDs typically approve investment plans in information security and privacy, so the existence of such plans signals BoDs' awareness of, and engagement, with this matter (people, processes and policies)	Schinagl and Shahim (2020)
		Total Infosec and privacy	Up to 0.5%; $0.5\% < x < 1.5\%$; $1.5\% < x < 2.5\%$; $2.5\% < x <$	As BoDs typically approve ICT and information security/	Institute of Directors New

Table A1.

(*continued*)

Action/ recommendation area	Recommendation category (Renaud *et al.*, 2019)	Variables (mapped from the survey)	Possible responses (from the survey)	Mapping rationale (and main focus: people, processes and policies)	Supporting literature
		expenditure/ ICT budget	3.5%; 3.5% $< x <$ 4.5%; 4.5% $< x <$ 6.5%; 6.5% $< x <$ 8.5%; 8.5% $< x <$ 10.5%; 10.5% $< x <$ 12.5%; 12.5% $< x <$ 14.5%; More than 14.5%; Doesn't know/ doesn't answer	privacy budgets, the size of a budget suggests a BoDs approval, signaling their perception of the need for expenditure (people, processes and policies)	Zealand (2018)
		Variation of Infosec and privacy budget in the last 12 months?	Decrease of more than 30%; Decrease between 20% and 30%; Decrease between 10% and 20%; Decrease up to 10%; Stable (variation between −1% and +1%); Increase between 1% and 5%; Increase between 5% and 10%; Increase between 10% and 20%; Increase between 20% and 30%; Increase of more than 30%; Not applicable (it was 0 in 2016)	An increase in these two budgets signals BoDs awareness of, and engagement with, information security and privacy (people, processes and policies)	Institute of Directors New Zealand (2018)
		Total variables included in the mapping: 7 Together, the above variables focus on an organisation's investment decisions to improve some of the people, policies and processes dimensions of information security; produce further data and information on the topic; and support the top organisational leaders in making such decisions			
Organisational culture	Monitor cyber-culture	Classroom training	Not done; Casual; Regular	Through interaction with peers and contents, regular classroom training is one acknowledged measure to promote and monitor a sound information security culture (processes)	Chang and Hawamdeh (2020), Trim and Upton (2013)
		Online course	Not done; Casual; Regular	Through the flexible diffusion of contents and/or communication with instructors/peers, online courses contribute in fostering a sound information security culture and monitoring its development (processes)	Corradini (2020)
		Informative materials (brochures)	Not done; Casual; Regular	Informative materials promote information security culture in a flexible way and leverage the power of visuals to raise viewers/ readers' engagement (processes)	Bilal (2011), He and Zhang (2019)

(*continued*)

Table A1.

Action/ recommendation area	Recommendation category (Renaud *et al.*, 2019)	Variables (mapped from the survey)	Possible responses (from the survey)	Mapping rationale (and main focus: people, processes and policies)	Supporting literature
		Informal meetings	Not done; Casual; Regular	Informal settings often promote frank conversations around information security, fostering a "no-blame" approach to the topic and enabling monitoring of its development (processes)	Corradini (2020)
		Email and newsletters	Not done; Casual; Regular	These tools can create a sense of urgency in viewers/readers to promote a sound information security culture in the organisation (processes)	Bilal (2011), Corradini (2020)
		Digital discussion boards (blogs)	Not done; Casual; Regular		Abawajy (2014)
		Self-assessment tests	Not done; Casual; Regular	As assessment pieces, these tools contribute in aggregating an organisation's approach towards information security culture (processes)	Esparza *et al.* (2020)
		Gamification	Not done; Casual; Regular	Imparting information security principles in a fun way, and often incorporating quizzes which help to assess current information security culture, this tool is a user-favourite and has gained traction in recent years (processes)	Abu-Amara *et al.* (2021), Van Steen and Deeleman (2021)
		Rewards	Not done; Casual; Regular	Rewards, even only public recognition, for information security behaviours help to engender an organisational information security culture and monitor its development over time (processes)	Bair *et al.* (2017)
		Phishing simulation	Not done; Casual; Regular	Phishing simulations are intended to raise information security awareness and consequently improve security culture. User performance can be easily monitored (processes)	Gordon *et al.* (2019), Williams *et al.* (2018)
		Training and awareness initiatives	Not done; Casual; Regular	Information security culture has its roots in awareness; these	Corradini (2020),

(*continued*)

Table A1.

Action/ recommendation area	Recommendation category (Renaud *et al.*, 2019)	Variables (mapped from the survey)	Possible responses (from the survey)	Mapping rationale (and main focus: people, processes and policies)	Supporting literature
				initiatives serve to nurture culture and enable monitoring of employees' performance in this field (processes)	Siponen (2001)
	Regular awareness training	Insufficient survey responses			
		Total variables included in the mapping: 11 Together, the above variables indicate an organisation's efforts in improving some of the processes associated with promoting a sound cybersecurity culture and monitoring it. The people, and policy dimensions are, however, absent from the mapping.			
Risk management and frameworks	Act to proactively detect intrusions (security) and mistakes (safety)	Classroom training	Not done; Casual; Regular	All of these tools and initiatives are likely to incorporate instructions on how to detect intrusion attempts (especially social engineering attacks). Employees are usually also encouraged to report their mistakes (e.g. clicking on a phishing message) in these training and awareness initiatives (processes)	Chang and Hawamdeh (2020), Trim and Upton (2013)
		Online course	Not done; Casual; Regular		Corradini (2020)
		Informal meetings	Not done; Casual; Regular		Corradini (2020)
		Email and newsletters	Not done; Casual; Regular		Bilal, (2011), Corradini (2020)
		Informative materials (brochures)	Not done; Casual; Regular		Bilal (2011), He and Zhang (2019)
		Self-assessment tests	Not done; Casual; Regular		Esparza *et al.* (2020)
		Gamification	Not done; Casual; Regular		Van Steen and Deeleman (2021)
		Rewards	Not done; Casual; Regular		Bair *et al.* (2017)
		Digital discussion boards (blogs)	Not done; Casual; Regular		Abawajy (2014)
		Phishing simulation	Not done; Casual; Regular		Gordon *et al.* (2019), Williams *et al.* (2018)
		Incident notification channel	Not done; Casual; Regular	Having a channel that employees can use to report incidents eases proactive reporting of both intrusions and mistakes (processes)	Briggs *et al.* (2017)

(*continued*)

Table A1.

Action/ recommendation area	Recommendation category (Renaud *et al.*, 2019)	Variables (mapped from the survey)	Possible responses (from the survey)	Mapping rationale (and main focus: people, processes and policies)	Supporting literature
		Threat identification	Someone else in charge; Occasionally involved; Responsible	This variable indicates whether organisational leaders in information security have, among their tasks, also threat identification. Taking personal responsibility in this field signals an organisation's proactive approach to detect intrusions and mistakes (people and processes)	Posthumus and Von Solms (2004)
		Ethical hackers: presence/in progress	Yes; No	If companies ae concerned about detecting intrusion attempts, engaging ethical hackers is a sign of proactivity in this area (people)	Wylie and Crawley (2021)
		Total variables included in the mapping: 13 Together, the above variables signal an organisation's investments and efforts in improving some of the people and processes dimensions associated with raising awareness among employees to proactively act to identify intrusions (security breaches) and mistakes (human error). The policies dimension is, however, absent from the mapping			
	Monitoring of new cyber/ physical risks, including knowledge risks	Information security assessment	Someone else in charge; Occasionally involved; Responsible	This variable indicates whether organisational leaders in information security have, among their tasks, also conducting information security assessment. Taking personal responsibility in this field signals an organisation's active monitoring of cyber/ physical risks, including risks associated with knowledge (people and processes)	Refsdal *et al.* (2015)
		Threat identification	Someone else in charge; Occasionally involved; Responsible	This variable indicates whether organisational leaders in information security have, among their tasks, also threat identification. Taking personal responsibility in this field signals an organisation's active monitoring of cyber/ physical risks, including risks associated with knowledge (people and processes)	Posthumus and Von Solms (2004)

(*continued*)

Table A1.

Action/ recommendation area	Recommendation category (Renaud *et al.*, 2019)	Variables (mapped from the survey)	Possible responses (from the survey)	Mapping rationale (and main focus: people, processes and policies)	Supporting literature
		Cyber risk analysis	Someone else in charge; Occasionally involved; Responsible	This variable indicates whether organisational leaders in information security have, among their tasks, also threat identification. Taking personal responsibility in this field signals an organisation's active monitoring of cyber/ physical risks, including risks associated with knowledge (people and processes)	Refsdal *et al.* (2015)
		Security analyst: presence/in progress	Yes; No	Absence of a security analyst signals an organisation's scarce attention to monitoring of cyber/physical risks, including risks associated with knowledge (people)	Refsdal *et al.* (2015)
		Definition of security policies and risk assessment	Not planned; Planned; In progress; Implemented	Having formulated these definitions suggests an organisational awareness of cyber/ physical and knowledge-related risk monitoring (policies and processes)	Von Solms and Von Solms (2008)
		Investment plan for information security and privacy? To what extent?	No, budgeting occurs on a contingency basis; Yes, an annual one; Yes, a multi-year one; Yes, a multi-year one included in the strategic plan	Investing in information security and privacy suggests that the organisation is active in monitoring cyber/ physical and knowledge-related risks (people, processes and policies)	Schatz and Bashroush (2017)
		Total variables included in the mapping: 6 Together, the above variables cover some of the people, policies and process dimensions associated with monitoring new cyber/physical risks, including knowledge risks			
	Select best information security mechanisms and associated standards (e.g. NIST)	Definition of security architecture Policy and security framework definition	Someone else in charge; Occasionally involved; Responsible Someone else in charge; Occasionally involved; Responsible	An organisational leader in information security in charge, among others, of the definition of the company's security architecture and of the company's policy and security framework signals the strategic value that the	Chang and Hawamdeh (2020) Tselios *et al.* (2020)

(*continued*)

Table A1.

Action/ recommendation area	Recommendation category (Renaud *et al.*, 2019)	Variables (mapped from the survey)	Possible responses (from the survey)	Mapping rationale (and main focus: people, processes and policies)	Supporting literature
				organisation attributes to this activity and is an essential stepping-stone for the implementation of the best mechanisms in information security (people, processes and policies)	
		Scouting of security products	Someone else in charge; Occasionally involved; Responsible	An organisational leader in information security in charge, among others, of the scouting of the best security products signals the strategic value that the organisation attributed to this activity and is an essential stepping-stone for the implementation of the best mechanisms in information security. This kind of proactivity and deliberate searching for products is a sign that the organisation is actively looking for the best security mechanisms (people)	Von Solms and Von Solms (2008)
		Security analyst: presence/in progress	Yes; No	The presence of these experts is an indication that the company is in a good position to select the best information security mechanisms (people).	Allen *et al.* (2015)
		Security administrator: presence/in progress	Yes; No		Allen *et al.* (2015)
		Security architect: presence/in progress	Yes; No		Allen *et al.* (2015)
		Security engineer: presence/in progress	Yes; No		
		Total variables included in the mapping: 7 Together, the above variables encompass some of the people (for the most part) and policies, and processes (in minor part) dimensions associated with selecting the best information security mechanisms and associated standards for the organisation			
Budget and insurance	Balanced and sustained information security spending	Insufficient survey responses			
	Take out cyber insurance	Insufficient survey responses			

(*continued*)

Table A1.

Action/ recommendation area	Recommendation category (Renaud *et al.*, 2019)	Variables (mapped from the survey)	Possible responses (from the survey)	Mapping rationale (and main focus: people, processes and policies)	Supporting literature
Cyber-response	Adopt a breach management plan	Communication of a personal data breach to the data subject	Yes; No	This component is an essential element of any breach management plan (policies and processes)	IT Governance Privacy Team (2020), Khan *et al.* (2021)
		Communication of personal data breach to the supervisory authority	Yes; No	This is a legal requirement in the country where this data was collected, so is an essential element of a breach management plan (policies and processes)	IT Governance Privacy Team (2020), Khan *et al.* (2021)
		Monitor GDPR Compliance	Yes; No	This is a legal requirement in the country where this data was collected, so is an essential element of a breach management plan (policies and processes)	IT Governance Privacy Team (2020)
		Total variables included in the mapping: 3 Together, the above variables signal an organisation's focus on adopting a breach management plan, with reference to policies and processes dimensions. The people dimension is, however, absent from the mapping			
	Appoint a rapid response team	Incident notification channel	Not done; Casual; Regular	Having an incident notification channel indicates a preparedness for responding to incidents (processes)	Briggs *et al.* (2017)
		Incident response	Someone else in charge; Occasionally involved; Responsible	An organisational leader in information security in charge, among others, of incident response signals the strategic value that the organisation attributes to this activity and is an essential stepping-stone for the appointment of a rapid response team (people)	Khan *et al.* (2021)
		Total variables included in the mapping: 2 Together, the above variables indicate an organisation's degree of preparedness in appointing a rapid response team. Mapped dimensions are people and processes, whilst the policies dimension is absent from the mapping			
Strategies and action plans	Formulate plans of actions and refresh them annually	Insufficient survey responses			
	Oversee plans of action, with appointment of	Insufficient survey responses			

(*continued*)

Table A1.

Action/ recommendation area	Recommendation category (Renaud *et al.*, 2019)	Variables (mapped from the survey)	Possible responses (from the survey)	Mapping rationale (and main focus: people, processes and policies)	Supporting literature
	key account manager				
	Adopt a business continuity plan				Insufficient survey responses
Supply chain management	Retain/hire consultants to assess cyber-governance mechanisms	Insufficient survey responses			
	Retain/hire lawyers for legal implications	Insufficient survey responses			
	Retain/hire expert company in cyber-response	Insufficient survey responses			
	Ensure stakeholder security practice	Insufficient survey responses			
	Assess information security measures of SHS/ vendors	Insufficient survey responses			
	Ensure contractors treat IC-information confidentially/ securely	Insufficient survey responses			
	Retain/hire cyber talent	Ethical hackers: presence/in progress	Yes; No	Having these professionals in residence indicates that cyber talent is being hired and retained by the organisation (people)	Le Blanc and Freeman (2016)
		Machine learning specialist: presence/in progress	Yes; No		Chen *et al.* (2021)
		Security administrator: presence/in progress	Yes; No		Allen *et al.* (2015)
		Security analyst: presence/in progress	Yes; No		Allen *et al.* (2015)
		Security architect: presence/in progress	Yes; No		Allen *et al.* (2015)
		Security developer: presence/in progress	Yes; No		Allen *et al.* (2015)
		Security engineer:	Yes; No		Allen *et al.* (2015)

(*continued*)

Table A1.

Action/ recommendation area	Recommendation category (Renaud *et al.*, 2019)	Variables (mapped from the survey)	Possible responses (from the survey)	Mapping rationale (and main focus: people, processes and policies)	Supporting literature
		presence/in progress			
		Total variables included in the mapping: 7			
		Together, the above variables signal an organisation's willingness to hire and retain cyber-talent. The processes and policies dimensions are technically absent, but can be derived from the people one (e.g. policies and processes to do so are likely in place if the organisation hires in the above positions)			
	Invest in ethical hacking	Ethical hackers: presence/in progress	Yes; No	Having these professionals in residence is evidence of an investment in ethical hacking (people)	Le Blanc and Freeman (2016), Wylie and Crawley (2021)
		Total variables included in the mapping: 1			
		The above variables signal an organisation's attention in investing in ethical hacking (people dimension mainly, with the possibility to implicitly derive the processes and policies dimensions)			
Asset management	Identify tangible and intangible organisational assets	Information security assessment	Someone else in charge; Occasionally involved; Responsible	An organisational leader in information security in charge, among others, of information security assessment signals the strategic value that the organisation attributes to this activity. Conducting an information security assessment incorporates the need to identify both tangible and intangible assets (people and processes)	Von Solms and Von Solms (2008)
		Investment plan for Information Security and Privacy? To what extent?	No, budgeting occurs on a contingency basis; Yes, an annual one; Yes, a multi-year one; Yes, a multi-year one included in the strategic plan	The establishment of an investment plan for information security and privacy is a stepping stone towards the identification of tangible and intangible organisational assets, to prioritise investments in this area (policies and processes)	Schatz and Bashroush (2017)
		Total variables included in the mapping: 2			
		Together, the above variables indicate an organisation's efforts in identifying tangible and intangible organisation assets (people, processes and policies dimensions)			
	Prioritise such assets for risk management purposes	Information security assessment	Someone else in charge; Occasionally involved; Responsible	An organisational leader in information security in charge, among others, of information security assessment signals the strategic value that the	Von Solms and Von Solms (2008)

(*continued*)

Table A1.

Action/ recommendation area	Recommendation category (Renaud *et al.*, 2019)	Variables (mapped from the survey)	Possible responses (from the survey)	Mapping rationale (and main focus: people, processes and policies)	Supporting literature
				organisation attributes to this activity. Conducting an information security assessment permits organisations to prioritise assets for risk management purposes (people and processes)	
		Investment plan for information security and privacy? To what extent?	No, budgeting occurs on a contingency basis; Yes, an annual one; Yes, a multi-year one; Yes, a multi-year one included in the strategic plan	The establishment of an investment plan for information security and privacy is a stepping stone towards the prioritisation of tangible and intangible organisational assets for risk management purposes, to prioritise investments in this area (policies and processes)	Schatz and Bashroush (2017)
		Total variables included in the mapping: 2 Together, the above variables indicate an organisation's attention to prioritise tangible and intangible assets for risk management purposes from a people, policies and processes dimension			
Information sharing	Organise organisational learning sessions post-emergency	Insufficient survey responses			
Others	Improve measures for the security of internet-related knowledge	Classroom training	Not done; Casual; Regular	All of these tools and initiatives raise employees' awareness in information security and, subsequently, increase the chances of improving measures for the security of internet-related knowledge (processes)	Sheng (2020)
		Online courses	Not done; Casual; Regular		Corradini (2020)
		Informal meetings	Not done; Casual; Regular		Corradini (2020)
		Email and newsletters	Not done; Casual; Regular		Bilal (2011), Corradini (2020)
		Informative materials (brochures)	Not done; Casual; Regular		Bilal (2011), He and Zhang (2019)
		Self-assessment tests	Not done; Casual; Regular		Esparza *et al.* (2020)
		Gamification	Not done; Casual; Regular		Van Steen and Deeleman (2021)
		Rewards	Not done; Casual; Regular		Bair *et al.* (2017)
		Digital discussion boards (blogs)	Not done; Casual; Regular		Abawajy (2014)
		Phishing simulation	Not done; Casual; Regular		Gordon *et al.* (2019),

(*continued*)

Table A1.

Action/ recommendation area	Recommendation category (Renaud *et al.*, 2019)	Variables (mapped from the survey)	Possible responses (from the survey)	Mapping rationale (and main focus: people, processes and policies)	Supporting literature
					Williams *et al.* (2018)
		Incident notification channel	Not done; Casual; Regular	An incident notification channel allows employees to signal intrusions and mistakes and is a stepping stone in the improvement of measures for the security of internet-related knowledge (processes)	Briggs *et al.* (2017)
		Total variables included in the mapping: 11			
		Together, the above variables demonstrate an organisation's efforts in improving measures for the security of internet-related knowledge, from the perspective of the processes dimension. The people and policies dimensions, however, are uncovered			

Table A1.

About the authors

Ivano Bongiovanni is a Lecturer in Information Security Governance and Leadership with the University of Queensland Business School. His research areas are cybersecurity management, design thinking and design-led innovation. He started his career in the Italian Police, and then became Deputy Venue Security Manager at the XX Winter Olympic Games (Turin). After a stint with the UN Conference on Disarmament (Geneva), he joined academia with Bocconi University. After his PhD at QUT (Brisbane), he worked as a Research Fellow with the Adam Smith Business School at the University of Glasgow. He holds MSc degrees from Bocconi University and Sciences-Po (Paris). Ivano Bongiovanni is the corresponding author and can be contacted at: i.bongiovanni@uq.edu.au

Karen Renaud is a Computing Scientist at the University of Strathclyde in Glasgow, working on all aspects of human-centred security and privacy. She was educated at the Universities of Pretoria, South Africa and Glasgow. Her research has been funded by the Association of Commonwealth Universities, the Royal Society, the Royal Academy of Engineers and the Fulbright Commission. She works on deploying behavioural science techniques to improve security behaviours, and on end-user privacy-preserving behaviours. Her research is multi-disciplinary, essentially learning from other, more established, fields and harnessing methods and techniques from other disciplines to understand and influence cybersecurity behaviours.

Humphrey Brydon is a Senior Lecturer at the University of the Western Cape. He is a Statistician at the University of the Western Cape. He completed his PhD (Statistics) at the University of the Western Cape in 2018. He has 7 years' experience in the academic environment and his research interests include missing data, the application of statistical learning methodologies and big data analytics.

Renette Blignaut is a Professor of Statistics at the University of the Western Cape. She was trained as Statistician by completing an MSc (Mathematical Statistics) at the University of Cape Town, and then completed a PhD (Statistics) at the University of Pretoria. Renette has eight years' experience as a Statistician and 29 years' experience in an academic environment, training students in the field of statistics and data science. Her research interests include statistical learning methods (including data mining), biostatistics, mobile security awareness and science education.

Angelo Cavallo is an Assistant Professor at Politecnico di Milano. His main research areas include Strategic Management, Entrepreneurship and Digital Transformation. His research interests are focused on entrepreneurial ecosystems, entrepreneurial dynamics and business modelling. He is member of the core faculty of MIP – Graduate School of Business, and Director of the Space Economy Observatory at Politecnico di Milano. He is author of journal articles (appearing in outlets such as *Journal of Business Research*, *Technological Forecasting and Social Change* and the *International Entrepreneurship and Management Journal*), book chapters and conference proceedings.