A Quantification Mechanism for Assessing Adherence to Information Security Governance Guidelines

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 utilising 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. We argue that such data could be repurposed to quantify adherence to existing information security guidelines, and we propose, and test, an original methodology to do so.

Design/Methodology/Approach: We 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. We test our quantification mechanism using a dataset 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 our 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 dataset to measure adherence.

Originality: To the best of our 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 published cyber security guidelines. This way, our mechanism responds to increasing calls for the adoption of research practices that minimise waste of resources and enhance research sustainability.

Keywords: Information security governance, cybersecurity, adherence quantification mechanism, information security guidelines, Boards of Directors, organisational leaders, survey.

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, Kaplan, & Van Der Oord, 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, Mellado, Fernández-Medina, & Mouratidis, 2015). Security solutions, such as the setup of a Security Operations Centre (SOC), or reliance on outsourced security, are impacted by factors such as maturity, size, and industry of the organisation, budget availability, legal requirements, etc. 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, Von Solms, & Von Solms, 2019; Zukis, 2016). Because organisations engage in social comparisons with their peers to decide which measures to implement (Barlette, Gundolf, & Jaouen, 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, Neveol, Daly, & Frenoux, 2020) has encouraged the re-use of existing research materials, as long as pertinent to the addressed research questions, in order to limit the waste of research resources. After all, novelty does not come only from new datasets, but also from the application of existing datasets 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, Von Solms, and Von

Solms (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 utilised by other researchers who face data scarcity around information security (Atapour-Abarghouei, McGough, & Wall, 2020); as for the latter, organisational leaders can employ 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 dataset 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 & Beaumont, 2017). However, the uplifting of information security "from the basement to the boardroom" (Schinagl & 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, Naegele, & Girod, 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 & 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 & 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 & Von Solms, 2018). Third, organisational structures may, at times, confine information security away from the reporting lines of BoDs: research shows that CIOs rarely report to CEOs, and are mostly not board members (Grobman & 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 (L. A. Gordon & Loeb, 2002) and what areas should be covered as a priority (Daniel Schatz & 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 & 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 a) standards, or *standard-like* frameworks/schemes and b) 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, Cherdantseva, Reinecke, & Burnap, 2020) and a human perspective (Zhang & Ghorbani, 2020). Internationally recognised standards such as ISO27001:2015, NIST, and 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 I).

---TABLE I HERE---

Overall, frameworks for information security governance suffer from flaws that can be broadly synthesised around the following points (Schinagl & 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.

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 BoDs

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*, despite undeniable advancements in this field, a traditional *technical-first* approach to information security is still widespread (Soomro, Shah, & Ahmed, 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, Von Solms, and Von Solms (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 II proposes a synthesis of the recommended interventions around 10 main areas.

---TABLE II HERE---

The effectiveness of evidence-based frameworks similar to the ones proposed by Zukis (2016) and Renaud, Von Solms, and Von Solms (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 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, Von Solms, and Von Solms (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

---FIGURE 1 HERE---

In our study, we formulated a quantification mechanism, which is composed of the following steps (Figure 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, Von Solms, and Von Solms (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, Von Solms, and Von Solms (2019), the mapped variables from the survey are presented in Table III. 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).

---TABLE III HERE---

Appendix A 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 utilised to measure adherence to the recommendations are, at best, proxies. To overcome this, we offer a point-by-point explanation of the rationale utilised for our mapping, equally contained in Appendix A (column: Mapping rationale).

Step 2) Data Cleaning & Preparation:

2a) Qualitative measures were converted to quantitative ones for statistical analysis. As an illustration, answers that could be attributed to a 5-point Likert scale (from 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).

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 due to missing proportions and allowed us to calculate the related score (Appendix A).

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.

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, Von Solms, and Von Solms (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, Von Solms, and Von Solms (2019).

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 & Energy, Public Administration and Healthcare, Finance (including banking and insurance), Telecommunications & 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, Von Solms and Von Solms (2019) (Table IV). The overall average level was calculated by an aggregation of the category scores using equal weighting.

---TABLE IV HERE---

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).

---FIGURE 2 HERE---

An analysis of the scores per industry (Table V) 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.

---TABLE V HERE---

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 & 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 x 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 x inter-quartile range.

---FIGURE 3 HERE---

Our analysis extended to include the adherence score for each recommendation in the adopted framework (Table V). 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 to 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 regards 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 VI would be a better reflection of the adherence level. A more detailed discussion of the results is given in the next section.

---TABLE VI HERE---

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.

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 & Sadath, 2019).

Other industries also demonstrated high adherence to the framework. Manufacturing and Utility & Energy (Figure 3) contained outlier observations above the 1.5 x 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 & Faily, 2017), this result highlights how, despite 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 & Zyngier, 2007), being that in the field of smart grids (Leszczyna, 2018), cyber-risk management (Collier et al., 2014), or cyber-response (Nespoli, Papamartzivanos, Gomez Marmol, & Kambourakis, 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, Renaud, & Cairns, 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, Almache-Cueva, Silva-Rabadão, Yevseyeva, & Basto-Fernandes, 2017), especially considering contextual factors such as resource scarcity, increased digital footprint (Aliyu, He, Yevseyeva, & Luo, 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, Dynes, & Chang, 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 datasets 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 & 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, Von Solms, and Von Solms (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, Von Solms, & Von Solms, 2019). Nonetheless, two elements make our approach valid nonetheless: first, organisations willing to utilise our method to benchmark themselves against competitors or other companies would need to agree on the variables utilised 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 dataset, our approach aligns with calls in the literature for more efficient and sustainable research practices.

Acknowledgements

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.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & information technology, 33*(3), 237-248.

Abu-Amara, F., Almansoori, R., Alharbi, S., Alharbi, M., & Alshehhi, A. (2021). A novel SETA-based gamification framework to raise cybersecurity awareness. *International Journal of Information Technology (Singapore)*. doi:10.1007/s41870-021-00760-5

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

Agyepong, E., Cherdantseva, Y., Reinecke, P., & Burnap, P. (2020). Challenges and performance metrics for security operations center analysts: a systematic review. *Journal of Cyber Security Technology, 4*(3), 125-152. doi:10.1080/23742917.2019.1698178

Aliyu, A., He, Y., Yevseyeva, I., & 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., & 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 & Security, 98*, 102003.

Atapour-Abarghouei, A., McGough, A. S., & 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., & Shostack, A. (2017). That was close: Reward reporting of cybersecurity near misses. *Colo. Tech. LJ, 16*, 327.

Barlette, Y., Gundolf, K., & Jaouen, A. (2017). CEOs' information security behavior in SMEs: Does ownership matter? *Systemes d'information management, 22*(3), 7-45.

Bilal, K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African journal of business management, 5*(26). doi:10.5897/AJBM11.067

Bongiovanni, I., Renaud, K., & Cairns, G. (2020). Securing intellectual capital: an exploratory study in Australian universities. *Journal of intellectual capital, 21*(3), 481-505. doi:10.1108/JIC-08-2019-0197

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

Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. (2016). A Framework for Information Security Governance and Management. *IT professional, 18*(2), 22-30. doi:10.1109/MITP.2016.27

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

Chen, X., Susilo, W., & Bertino, E. (2021). *Cyber security meets machine learning*. Singapore: Springer.

Clair, N. S., & Girard, J. (2020). Are Cybersecurity Professionals Satisfied with Recent Cybersecurity Graduates? *Journal of The Colloquium for Information Systems Security Education, 7*(1), 7-7.

Collier, Z. A., DiMase, D., Walters, S., Tehranipoor, M. M., Lambert, J. H., & Linkov, I. (2014). Cybersecurity Standards: Managing Risk and Creating Resilience. *Computer, 47*(9), 70-76. doi:10.1109/mc.2013.448

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

Cyriac, N. T., & Sadath, L. (2019, 21-22 November). *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, India.
Damenu, T. K., & Beaumont, C. (2017). Analysing information security in a bank using soft systems methodology. *Information and Computer Security, 25*(3), 240-258. doi:10.1108/ICS-07-2016-0053
Dutta, A., & McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review, 45*(1), 67-87. doi:10.2307/41166154
Esparza, J., Caporusso, N., & Walters, A. (2020). Advances in Human Factors in Cybersecurity. In (Vol. 1219, pp. 88-94). Cham: Springer International Publishing.
Fitzgerald, T. (2012). *Information security governance simplified from the boardroom to the keyboard* (1st edition ed.). Boca Raton: Fla: CRC Press.
Gordon, L. A., & Loeb, M. P. (2002). Return on information security investments: Myths vs. Realities. *Strategic finance, 84*(5), 26.
Gordon, W. J., Wright, A., Glynn, R. J., Kadakia, J., Mazzone, C., Leinbach, E., & 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, 26*(6), 547-552.
Goss, D. D. (2017). Operationalizing Cybersecurity—Framing Efforts to Secure US Information Systems. *The Cyber Defense Review, 2*(2), 91-110.
Graves, J. (2019). Reactive vs. proactive cybersecurity: 5 reasons why traditional security no longer works. Retrieved from https://www.fortinet.com/blog/industry-trends/reactive-vs--proactive-cybersecurity--5-reasons-why-traditional
Grobman, S., & Cerra, A. (2016). *The Second Economy: The Race for Trust, Treasure and Time in the Cybersecurity War*. Berkeley, CA: Apress.
Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). A process framework for information security management. *International journal of information systems and project management, 4*(4), 27-47. doi:10.12821/ijispm040402
He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of organizational computing and electronic commerce, 29*(4), 249-257. doi:10.1080/10919392.2019.1611528
Hoppmann, J., Naegele, F., & 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, 62*(2), 437-468. doi:10.5465/amj.2016.1091
Ilvonen, I. (2013). *Knowledge security-a conceptual analysis*. Tampere University, Tampere, Finland. Retrieved from https://trepo.tuni.fi/handle/10024/114659
Institute of Directors New Zealand. (2018). *Reporting cybersecurity to boards*. Retrieved from 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.). Rolling Meadows, IL: IT Governance Institute.
IT Governance Privacy Team. (2020). *EU General Data Protection Regulation (GDPR) – An implementation and compliance guide, fourth edition*: IT Governance Publishing.
Jennex, M. E., & Zyngier, S. (2007). Security as a contributor to knowledge management success. *Information Systems Frontiers, 9*(5), 493-504. doi:10.1007/s10796-007-9053-4
Kauspadiene, L., Cenys, A., Goranin, N., Tjoa, S., & Ramanauskaite, S. (2017). High-Level Self-Sustaining Information Security Management Framework. *Baltic Journal of Modern Computing, 5*(1), 107. doi:10.22364/bjmc.2017.5.1.07
Khan, F., Kim, J. H., Mathiassen, L., & Moore, R. (2021). Data breach management: An integrated risk model. *Information & Management, 58*(1), 103392. doi:10.1016/j.im.2020.103392

Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *Computers & Security, 70*, 663-674. doi:10.1016/j.cose.2017.08.001

Klein, A., Manini, R., & Shi, Y. (2020). Across the Pond: How U.S. Firms' Boards of Directors Adapted to the Passage of the GDPR. *SSRN*. doi:http://dx.doi.org/10.2139/ssrn.3640515

Knapp, K. J., Franklin Morris, R., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security, 28*(7), 493-508. doi:10.1016/j.cose.2009.07.001

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

Leszczyna, R. (2018). A review of standards with cybersecurity requirements for smart grid. *Computers & Security, 77*, 262-276. doi:10.1016/j.cose.2018.03.011

Ligozat, A.-L., Neveol, A., Daly, B., & Frenoux, E. (2020). Ten simple rules to make your research more sustainable. *PLoS computational biology, 16*(9). doi:10.1371/journal.pcbi.1008148

Maleh, Y., Ezzati, A., Sahid, A., & Belaissaoui, M. (2017). CAFISGO: a Capability Assessment Framework for Information Security Governance in Organizations. *Journal of Information Assurance Security, 12*(6).

Merrick, R., & 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, 66*(3), 38.

Mishra, S. (2015). Organizational objectives for information security governance: a value focused assessment. *Information & Computer Security, 23*(2), 122-144.

Moore, T., Dynes, S., & Chang, F. (2015). Identifying how firms manage cybersecurity investment. 32. Retrieved from 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., & Kambourakis, G. (2018). Optimal Countermeasures Selection Against Cyber Attacks: A Comprehensive Survey on Reaction Frameworks. *IEEE Communications surveys and tutorials, 20*(2), 1361-1396. doi:10.1109/COMST.2017.2781126

Nicho, M. (2018). A process model for implementing information systems security governance. *Information and Computer Security, 26*(1), 10-38. doi:10.1108/ICS-07-2016-0061

Nolan, R., & McFarlan, F. W. (2005). Information technology and the board of directors. *Harv Bus Rev, 83*(10), 96-157.

Park, H., Kim, S., & 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., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security, 23*(8), 638-646. doi:10.1016/j.cose.2004.10.006

PwC. (2012). *Bridging the IT confidence gap (abridged version)*. Retrieved from New York:

Rebollo, O., Mellado, D., & Fernandez-Medina, E. (2015). ISGcloud: a Security Governance Framework for Cloud Computing. *Computer journal, 58*(10), 2233-2254. doi:10.1093/comjnl/bxu141

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

Redmiles, E. M., Warford, N., Jayanti, A., Koneru, A., Kross, S., Morales, M., . . . Mazurek, M. L. (2020, 12-14 August). *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.

Redseal. (2016). *The Rise of Cyber-Overconfidence in C-Suite*. Retrieved from https://www.redseal.net/wp-content/uploads/2016/12/RedSeal-CEO-Survey-Executive-Summary.pdf

Refsdal, A., Solhaug, B., & Stølen, K. (2015). *Cyber-Risk Management* (1st ed. 2015. ed.). Cham: Springer International Publishing : Imprint: Springer.
Renaud, K., Von Solms, B., & Von Solms, R. (2019). How does intellectual capital align with cyber security? *Journal of intellectual capital, 20*(5), 621-641. doi:10.1108/JIC-04-2019-0079
Roldán-Molina, G., Almache-Cueva, M., Silva-Rabadão, C., Yevseyeva, I., & Basto-Fernandes, V. (2017). A comparison of cybersecurity risk analysis tools. *Procedia computer science, 121*, 568-575.
Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review, 59*(2), 12-15.
Ruan, K. (2019). *Digital asset valuation and cyber risk measurement : principles of cybernomics*. London
London, England: Academic Press.
Saneei Moghadam, R., & Colomo-Palacios, R. (2018). Information security governance in big data environments: A systematic mapping. doi:10.1016/j.procs.2018.10.057
Schatz, D., & Bashroush, R. (2017). Economic valuation for information security investment: a systematic literature review. *Information Systems Frontiers, 19*(5), 1205-1228. doi:10.1007/s10796-016-9648-8
Schatz, D., & Bashroush, R. (2018). Corporate information security investment decisions: a qualitative data analysis approach. *International Journal of Enterprise Information Systems, 14*(2), 1-20.
Schinagl, S., & 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, 28*(2), 261-292.
Scully, T. (2014). The cyber security threat stops in the boardroom. *Journal of Business Continuity & Emergency Planning, 7*(2), 138-148.
Sheng, Q.-w. (2020). e-Learning, e-Education, and Online Training. In (Vol. 340, pp. 25-37). Cham: Springer International Publishing.
Siponen, M. T. (2001). Five dimensions of information security awareness. *Computers and Society, 31*(2), 24-29. doi:10.1145/503345.503348
Sobers, R. (2021). 134 Cyber security Statistics and Trends for 2021. Retrieved from https://www.varonis.com/blog/cybersecurity-statistics/
Soomro, Z., Shah, M., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT, 36*(2), 215-225. doi:10.1016/j.ijinfomgt.2015.11.009
Teplinsky, M. (2013). Fiddling On The Roof: Recent Developments In Cybersecurity. *American University Business Law Review, 2*(2), 225.
Trim, P., & Upton, D. (2013). *Cyber Security Culture*. Farnham: Routledge.
Tselios, C., Tsolis, G., & Athanatos, M. (2020). Computer Security. In (Vol. 11981, pp. 3-18). Cham: Springer International Publishing.
UK Government. (2020). Cyber Security Breaches Survey 2020. Retrieved from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020
Valentine, E. L. H., & Stewart, G. (2013). The emerging role of the Board of Directors in enterprise business technology governance. *International journal of disclosure and governance, 10*(4), 346-362. doi:10.1057/jdg.2013.11
Van Steen, T., & Deeleman, J. (2021). Successful Gamification of Cybersecurity Training. *Cyberpsychology, behavior and social networking, 24*(9), 593-598. doi:10.1089/cyber.2020.0526
Veiga, A. D., & Eloff, J. H. P. (2007). An Information Security Governance Framework. *Information systems management, 24*(4), 361-372. doi:10.1080/10580530701586136
Von Solms, B. (2006). Information Security – The Fourth Wave. *Computers & Security, 25*(3), 165-168. doi:10.1016/j.cose.2006.03.004
Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security–what goes where? *Information & Computer Security, 26*(1), 2-9.

Von Solms, R., & Von Solms, B. (2006). Information security governance: Due care. *Computers & Security, 25*(7), 494-497. doi:10.1016/j.cose.2006.08.013

Von Solms, S., & Von Solms, R. (2008). *Information security governance*: Springer Science & Business Media.

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International journal of human-computer studies, 120*, 1-13.

Wylie, P. L., & Crawley, K. (2021). *The pentester blueprint : starting a career as an ethical hacker*. Indianapolis, IN: John Wiley.

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

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

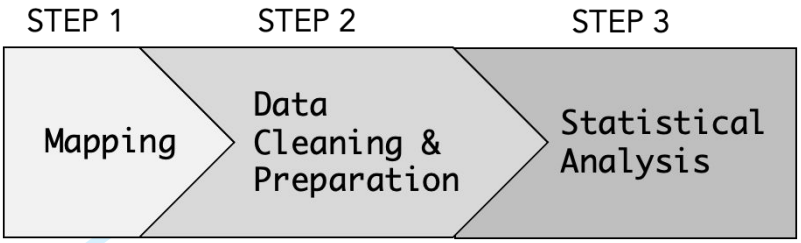


Figure 1: Adopted methodology

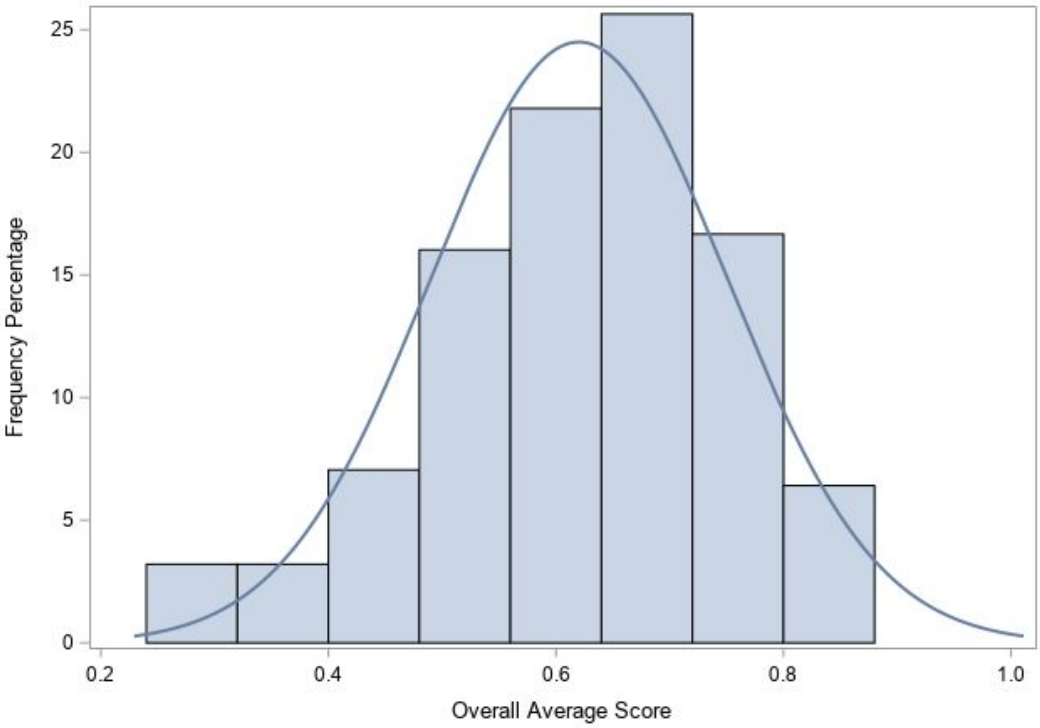
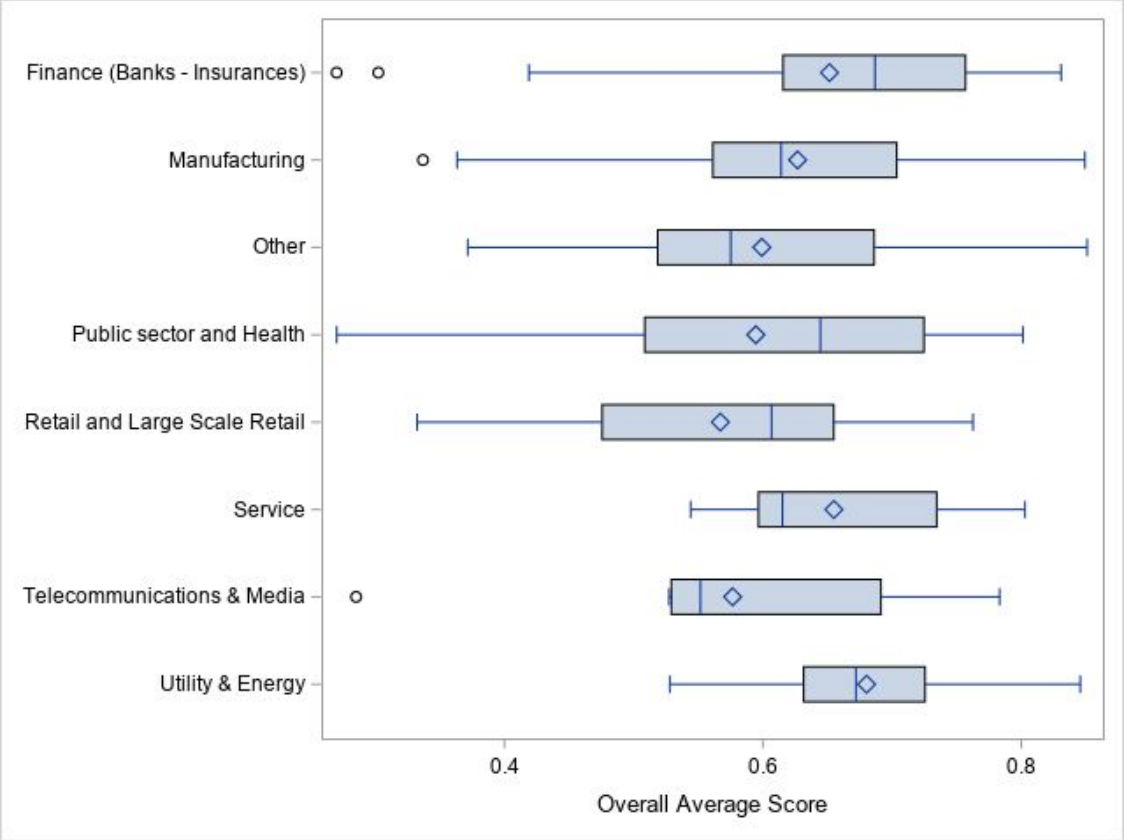


Figure 2: Distribution of adherence scores across the sample (n=156)



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

Figure 3: Overall average adherence score per industry

Table I: Information security governance frameworks

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 & Von Solms, 2004)	(Dutta & McCrohan, 2002)	(Knapp, Franklin Morris, Marshall, & Byrd, 2009)	(Kauspadiene, Cenys, Goranin, Tjoa, & Ramanauskaite, 2017)
NIST Cyberframework	(Von Solms & Von Solms, 2006)	(Veiga & Eloff, 2007)	(Haufe, Colomo-Palacios, Dzombeta, Brandis, & Stantchev, 2016)	(Rebollo, Mellado, & Fernandez-Medina, 2015)
COBIT	(Park, Kim, & Lee, 2006)	(Maleh, Ezzati, Sahid, & Belaissaoui, 2017)	(Carcary, Renaud, McLaughlin, & O'Brien, 2016)	(Saneei Moghadam & Colomo-Palacios, 2018)
ITIL			(Nicho, 2018)	

Table II: Practical recommendations for organisational leaders (from Zukis (2016) and Renaud, Von Solms, and Von Solms, (2019)

Action/ Recommendation Area	**Zukis (2016)**	**Renaud, Von Solms & Von Solms (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 cyber security 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

Action/ Recommendation Area	**Zukis (2016)**	**Renaud, Von Solms & Von Solms (2019)**
		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
		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 III: 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	Someone else in charge; Occasionally involved; Responsible	The CISO's involvement with the three listed activities indicates how cyber security leadership in the organisation engages in the selection of the best cybersecurity mechanisms and associated standards	(Chang & Hawamdeh, 2020)
	Scouting of security products			(Tselios, Tsolis, & Athanatos, 2020)
	Policy and security framework definition			(Von Solms & Von Solms, 2008)
	Question (from the survey): ***Does your company have individuals in the following job positions?***			
	Security administrator	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)
	Security analyst			(Allen et al., 2015)
	Security architect			(Allen et al., 2015)
	Security engineer			(Allen et al., 2015)
	Total variables included in the mapping: 7			

Table IV: Overall average adherence score

Number of observations	Average	Min	Max	Lower 95%	Upper 95%
156	0.620	0.270	0.851	0.600	0.641

Table V: Average and 95% confidence interval (CI) adherence score per industry

Industry	Number 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 & Media	8	0.577	0.285	0.783	0.445	0.709
Utility & Energy	12	0.680	0.528	0.846	0.629	0.732

Table VI: Overall Average Score by Recommendation Category

Recommendation category	Number 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