Insider Threats to Cyber Security in an Audit Environment

Admire Njowa, Belinda Schutte, and Zaakir Ally

Abstract There has been a notable increase in insider threats to information security (IS) globally. South African entities have thus not been spared, and the challenges relating to insider information security threats affect firms of all sizes and in all industries. It therefore follows that audit firms are not immune, as these rely on the trust given to them by their clients to keep their information secure. This is therefore a growing problem that has not spared entities in South Africa. The current study sought to evaluate the level of awareness and measures to safeguard client information from cyber related risks that emanate from within. The study employed a positivist research philosophy and a descriptive survey which focused on small to medium audit firms. A questionnaire was used for collecting data, which were analysed using descriptive statistical analysis. Findings showed that there was generally a high level of awareness amongst staff in the firms studied. Most firms have implemented suitable and relevant measures to safeguard client data electronically stored and or transmitted. Results also showed that most of the best practices utilised globally have been adopted in the audit firms under study. These include secure access methods like Virtual Private Network (VPN), internal firewalls, USB port locking, hard drive and memory stick encryption and the use of strong passwords. It was recommended that regulators and policy makers strive to provide the necessary guidance concerning client information security optimisation amongst audit firms, thus standardising this aspect and encouraging the adoption of best practices.

Keywords Cyber security · Insider threat · Awareness · Information security

A. Njowa (✉) · B. Schutte · Z. Ally
University of Johannesburg, Johannesburg, South Africa
e-mail: belindas@uj.ac.za; zaakira@uj.ac.za

T. Moloi, B. George (eds.), *Towards Digitally Transforming Accounting and Business Processes*, Springer Proceedings in Business and Economics,
https://doi.org/10.1007/978-3-031-46177-4_21

1 Introduction

Information is a critical asset in the efficient application and management of firm resources, and safeguarding this information remains a top priority for organisations globally (Rosati et al., 2019). Solms (2021) notes that cybercrime in South Africa has resulted in annual losses of up to R2.2 billion. Similarly, the South African Banking Risk Information Centre (SABRIC) (2021) reported that South Africa loses R2.4 billion to cyber-attacks annually. These entities included government agencies, medical institutions, financial institutions, and corporate institutions. Challenges relating to abuse of access privileges by internal users were one of the most prevalent forms of cyber security issues (Fagerström, 2013). Similarly, the prevalence of insider attacks is emphasised by Upton and Creese (2014) who state that there is an enormous number of about 80 million insider attacks in the United States that are happening annually, which number is likely higher as a lot of those attacks go unreported and undisclosed to protect organisation's reputations. The Audit Analytics Cyber Security Reports (2020) states that in most cases audit firms do not disclose the form of cyber-attack or the actual extent of data breaches to prevent reputational damage.

Audit firms are not immune to cyber security threats. This is more so given that audit firms' business is predicated on information collected, processed and stored. Thus, like any other organisations, audit firms face cyber security risk. The negative effects of cyber security breaches at both firm and market level are well documented (Spanos & Angelis, 2016; Rosati et al., 2017; Kamiya et al., 2018). Cyber security issues in audit firms are a typical case of issues that affect external stakeholders in the form of clients whose data is at risk (Hovav & Gray, 2014). However, little has been done by way of research of cyber security issues in small and medium audit firms, more so focusing on internal threats.

2 Literature Review

Existing literature on Information Security (IS) and related threats shows that information is an important resource in an organisation; therefore, safeguarding this information remains a top priority for organisations globally. This is more so given to the noted increase in the prevalence of IS threats globally. The upsurge in these threats and attacks is a great concern for entities in South Africa and abroad (Cheng et al., 2019). Despite notably little literature on audit firms and the problem of insider threats, it makes sense that they may not have been spared particularly given that they are entrusted with large volumes of client data. It is therefore important that the existing literature and knowledge on insider threats to IS reviewed to gain insights on what other writers have put forward on the subject matter. In the same vein, reviewing literature is important in locating the current study on audit firms within the current discourse on insider threats.

The term cyber security has attracted great interest in both academia and practice. This may explain the broad use of the terms as well as the variations in definitions attached to it. Cyber security has gained prominence as an information technology (IT) risk. However, it is only recently that such breaches and attacks have drawn great attention from both academics and practitioners. The Ponemon Institute (2017) reports that cyber-crime costs US$11.7 million per firm on average and that there have been a 27.4% increase in security breaches globally.

The definitions utilised in extant literature are context-bound, sometimes uninformative, and often subjective. There is thus no universally accepted definition of cyber security in extant literature. Seemma et al. (2018) define cyber security as the organisation of processes, resources, and structures utilised in protecting cyberspace and cyberspace-based systems. The definition is highly vague, leaving out important aspects which are better specifically mentioned. Canongia and Mandarino (2014) define cyber security as the art of ensuring the continuity and existence of the information society of a nation, protecting and guaranteeing its information, assets, and critical infrastructure in cyberspace. The definition demonstrates a higher order orientation by focusing on a nation as opposed to the lower order units like firms.

This study adopts the definition by Public Safety Canada (2014), which defines cybersecurity as the body of technologies, practices, processes and response and mitigation measures that are designed to protect computers, programs, networks and data from damage, attack or unauthorised access with a view to ensure integrity, confidentiality and availability. This definition is comprehensive, unifying and meaningful, and encapsulates all the important elements of cyber security. The emphasis of cyber security has historically been on servers, data, networks, services, and data processes. The user has however become the weakest link in recent times in the cyber security chain. This has manifested as privileged account misuse by individuals to whom access is granted. It is therefore important to place increased focus on the user behaviour analytics over a given set of cyber assets including aspects like encryption, access management, identity management as well as artificial intelligence use (Dunn & Egloff, 2016).

The nature of business globally has been altered by the propagation of network-based communications. This has brought an unprecedented level of vulnerabilities and threats to information systems within businesses. IS theories show that within modern business, internal employee behaviour can cause serious damage to information systems (Cooper et al., 2017). Aytes and Connolly's (2003) user behaviour model places emphasis on user perception of choice as well as risk, indicating that internal employee behaviour in the context of IS results from choices that they make. The implications of such behaviours are however sometimes organisation wide.

In recent times, there has been an increased dependence on entities on information as well as computing systems which they have used to anchor their business processes and activities including strategic planning. However, ISA came with the need to ensure that data and information are secure (Brodin, 2019). This is important in the context of the current study given that when a firm loses client information or control over the same, it suffers a loss of trust amongst its customers (Peters et al., 2017).

The balanced security controls approach has been widely accepted as a standard in the management of IS. There has been emphasis on technical solutions, and these have been identified at operational level in the context of IS and cyber security (Singh, 2013). Earlier research studies dominated by computer scientists like Jemal (2014); Kabanda (2018); and Khan (2019) focused on the development and configuration of technical security countermeasures with a view to improving protection and detection at operational level.

Literature on the trends in cyber-attacks and data breaches in organisations was also reviewed, and it is clear that cases have been on the rise and there has been great interest in academia and industry shown by the large amount of literature on these breaches. Furthermore, it has been considered in past studies though most of the literature is generic and falls short of analysing ISP in the context of audit firms.

3 Research Problem

There has been a spike in insider threats to data and IS globally. South Africa has not been spared as the problem has reared its ugly head, with local entities facing huge losses. The Cost of Insider Threats: Global Report conducted by the Ponemon Institute (2017) states that insider threat incidents have risen by 44% over the past 2 years, with the cost per incident up by more than a third to $15.38 million. More specifically Hurwitz (2020) demonstrates that 10% of surveyed entities have suffered financial losses due to insider IS threats. Equally, PwC (2021) reports an upsurge in insider information attacks amongst South African entities. South African entities have thus not been spared the challenges relating to insider IS threats. This is therefore a growing problem that has not spared entities in South Africa.

Accounting firms of all sizes rely on the trust given to them by their clients to keep their information secure. Firms are at a high risk of targeted data attacks because of valuable and sensitive data that they process, collaborate, and store. With the current wave of cyber related attacks, it is imperative for audit firms to ensure the Confidentiality Integrity and Availability (CIA) of client data as the improper handling of such information has serious repercussions to the audit firm and the client being audited. The audit profession has been under immense scrutiny because of several adverse findings against some major role players in the industry. Any issue or incident caused by an employee could cause an irreparable harm to the profession and the organisation.

4 Research Objectives

The objectives of this study were to:

i. Determine the level of awareness among small to medium audit firms' trainees and auditors in respect of cyber related risk to client's confidential information that they handle or transmit during and after audit engagements;
ii. Critically evaluate the perceptions on relevance and effectiveness of measures or strategies being utilised in these firms to safeguard electronically stored and transmitted client data; and
iii. Assess the measures implemented in small to medium audit firms against widely accepted industry standards and frameworks.

5 Research Methodology

The study is a descriptive study that utilised quantitative research methods to allow the researcher to reach a desired requirement of the study (Johnson, 2016). The study population included employees at all levels of small to medium audit firms in South Africa. A sample was selected using convenient sampling and this was meant to address access issues that could hinder progress in data collection. A questionnaire was used in collecting data to ensure the validity of findings. Descriptive statistical analysis and content analysis using Statistical Package for Social Science (SPSS) software were used in carrying out data analysis. The findings of the study were presented through tables.

6 Research Philosophy

There are two main research philosophies, namely the positivist and the interpretivist. The former sees a researcher assumes the role of a neutral and objective analyst (Ryan, 2018). A researcher thus makes detached interpretations regarding collected research data. Then, the interpretivist philosophy views reality as a social construct and, as such, there may be different interpretations attached to the same philosophy depending on people's experiences and beliefs (Ryan, 2018). Thus, people make sense of their environment through interpretation and meaning. The current study adopted a positivist research philosophy in which the researcher adopted the role of an independent analyst. This allowed the researcher to address all the stated objectives of the study. This philosophy sets the stage for usage of quantitative-method research paradigm in addressing the stated questions.

7 Research Design

Research design is commonly used when a study seeks to give a full description of the behaviour, problem or concept in its natural setting. The study undertakes a descriptive survey research design. A research design offers a framework which stipulates the kind of data that is to be collected, data collection procedure as well as data sources (Churchill & Lacobucci, 2005; Ramirez, 2017). The same was viewed as being the most appropriate in the current study as it allowed the researcher to acquire a great deal of information regarding the IS breaches by insiders. Furthermore, the design allowed the researcher leeway to analyse data provided by the research participants regarding the problem under study. According to Mugenda and Mugenda (2003), such research aims to give a description of the way things really are and such a research study provides a clear picture of the study population's status. The design was opted for as it allowed the researcher to make use of quantitative methods. In the same vein, the design allowed the researcher to gain a full and clear understanding of IS issues under study in the context of audit firms.

8 Research Approach

There are basically two main research approaches, and these are the deductive and inductive approaches. The former aims to explain causal relationships between variables and involves the development of hypotheses that are tested through gathering of primary data (Woiceshyn & Daellenbach, 2018). Such concepts must be operationalised in a manner that permits measurement to be done quantitatively. The latter places emphasis on collection of qualitative data. In this case, theory follows data. It is thus highly subjective from the perspective of the researcher, which may pose reliability challenges (Mwangi, 2017). The current study adopted a deductive research approach. This set the stage for the use of quantitative-methods research. This is opted for as it stresses numerical analysis as well as objectivity, replication and reliability. The study focused on factors influencing organisational commitment, which brings in a causal dimension.

9 Target Population

Target population relates to the totality of elements, cases or individuals that have a common trait that is of interest to a given study. The current study targeted small to medium audit firms in South Africa. Small to medium sized firms were opted for given that there has been a shift in the market in which big corporates now also engage the services of smaller to medium sized firms which are not part of the traditional 'big four' firms.

The sampling frame was limited to small and medium sized firms in South Africa. The study selected a sample of firms from the identified frame. Respondents were then selected randomly as the questionnaire was distributed to firms through training officers as a way of reaching all employee levels.

10 Research Instruments

The researcher employed a structured questionnaire in collecting data in the current study. This form of questionnaire was used for all the selected research participants. A questionnaire can be understood to be a specially designed form containing questions to which a participant should provide responses. A structured questionnaire contains both close-ended and open-ended questions. The current study utilised a likert scale questionnaire that had five sections. The first section contained questions on participants' and firms' profiles. The subsequent sections contained questions that addressed the stated research questions. Furthermore, each section contained a question with a 5-point scale (1 = Strongly disagree; 5 = Strongly agree). Each of the constructs carried propositions and assertions based on the literature reviewed. The propositions were drawn from literature on each of the research objectives. The questionnaire was opted for given that it is relatively less time consuming and cost effective. Furthermore, it is a widely used data collection instrument that is robust and straight-forward. The researcher also wanted to ensure that respondents could respond to questions when it was convenient for them to do so. Furthermore, the researcher was in a position to collect sufficient data from various locations without necessarily being there physically. Teddlie and Tashakkori (2004) indicate that the instrument allows a researcher to collect a lot of data in the shortest possible time. The structured questionnaire also helped ensure focus was maintained by limiting the scope of the data that could be provided while at the same time allowing respondents a little room to manoeuvre.

11 Ethical Considerations

The following steps were taken to ensure adherence with ethical principles in research:

- The researcher ensured that all respondents made conscious and informed decisions regarding their participation in the study. This was ensured through full disclosure of material facts about the study as well as the condition under which they would participate in the study.
- No respondent was coerced into participating in the study.

- The researcher treated all the collected data with utmost confidentiality and data were kept in a safe throughout the duration of the study. No data were divulged to any third party without the express consent of all the respondents.
- No visible connection was kept between the data collected and the individuals from whom the data were collected. This was in line with the undertaking to ensure anonymity of the participants.

12 Data Analysis and Presentation Tools

This relates to the work that is undertaken on research data to give it meaning and structure. Thus, this process may involve breaking down the data, organising it, capturing it as well as searching for meaning and patterns that address the stated research questions (Bogdan & Biklen, 2003). In the current study, the researcher utilised descriptive statistical analysis in analysing collected data. Descriptive statistics allowed the researcher to effectively summarise large volumes of data and analyse and present it effectively. The researcher presents findings using tables and this was opted for because they serve as visual aids to enhance the understanding by the audience. The main data analysis tool was SPSS.

13 Data Presentation and Analysis

Based on the below, 152 of the 160 that the researcher distributed were returned. However, 3 of these were unusable as they had missing data leaving the researcher with 149 fully usable instruments. The response rate was thus 93.1%. This is a high response rate, which means that the study was completed based on sufficient data collected from the identified and included individual auditors (Table 1).

Table 1 Response rate

Instrument	Distributed	Returned	Unusable	Response rate based on all returned (%)	Response rate based on usable questionnaires (%)
Structured questionnaire	160	152	3	95	93.1
Total	160	152	3	95	93.1

Source: Primary data

14 Respondent Profiles

The researcher sought to elicit certain relevant information about the respondents. This information was deemed relevant to the study and respondents were required to provide indications relating to the same. The researcher sought to determine the designation of the respondents in the study. Pursuant to this, each respondent was required to indicate their designation in their organisation. This was important in ascertaining whether the study achieved some balance regarding the distribution of individuals according to designations, which was estimated to lend credence to the findings of the study. Results are shown in Table 2 below.

Based on the results in the table above, 71.1% of the respondents were trainees while another 23.5% were managers. The remaining 5.4% were executives within their respective firms. This means that the study was able to cover all designations with regards to auditors included in the study. On the other hand, the researcher asked respondents to indicate the department in which they served. This was also important in assessing whether balance was achieved in this regard. Results are shown in Table 3 below.

Results indicate that 63.1% of the respondents served in the audit department while another 26.2% served in the Tax department. The remainder (10.7%) served in the.

IT audit department. The results thus show that all the departments of interest were covered in terms of sample selection. This is important in ensuring that any departmental differences are fully reflected in the findings of the study.

Table 2 Respondent designation

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Trainee	106	71.1	71.1	71.1
	Management	35	23.5	23.5	94.6
	Executive	8	5.4	5.4	100.0
	Total	149	100.0	100.0	

Source: Primary data

Table 3 Respondents' department

		Frequency	Percent	Valid percent	Cumulative percent
	Audit	94	63.1	63.1	63.1
	Tax	39	26.2	26.2	89.3
	IT audit	16	10.7	10.7	100.0
	Total	149	100.0	100.0	

Source: Primary data

15 Level of Awareness among Small to Medium Audit Firms' Trainees and Auditors in Respect of Cyber Related Risk to Confidential Client Information

This was the first stated objective of the study. It relates to the level of awareness of both auditors and trainees concerning the cybersecurity risks to client data. To address this objective, the research made some propositions based on literature reviewed. Respondents were expected to indicate the extent to which they agreed with the propositions on a 5-point Likert scale. A mean score of 3.5 and above signalled at least an agreement whilst a mean of between 2.6 and 3.4 signalled uncertainty. A means response of between 1 and 2.4 signalled at least a disagreement. The maximum response on the Likert scale and the minimum received are also included in the results presented in Table 4 below.

Results indicate that respondents had full knowledge of firm ISPs. This was the view shared by most of the respondents in the study, and the mean response of 3.94 indicates that most of the respondents were at least in agreement with the proposition by the researcher. The standard deviation for this item was 0.799, which is low. The low standard deviation indicates low variability of responses and high reliability of the mean. The high degree of awareness in this regard may be attributable to the efforts that firms make in a bid to ensure that there is awareness amongst employees.

Table 4 Level of awareness amounts trainees and auditors in medium-sized audit firms

	Responses	Minimum	Maximum	Mean	Std deviation
I have full knowledge of the firm's information security policy(s)	149	1	5	3.94	.799
I am able to identify phishing emails or links and always avoid or delete them.	149	2	5	4.44	.701
I am interested in the firm's information security and I am aware of the various cybersecurity risks and threats	149	1	5	4.02	.809
As an employee I am aware that client's information should always be kept confidential	149	1	5	4.89	.445
There is no problem with discussing audit matters when out with friends or using public transport.	149	1	5	1.39	.860
Client's information should never be shared with anyone who is not part of that particular task.	149	1	5	4.45	.926
Pop up messages whilst online are good as I do not miss out on specials.	149	1	5	1.60	.855

Source: Primary data

The study results also show that most of the respondents indicated that they were in a position to identify phishing emails or links and always avoided or deleted them. A mean score of 4.44 was recorded for this item while the standard deviation was 0.701. The mean score indicates that most of the respondents agreed with the researcher's statement while the standard deviation indicates that the mean score was highly reliable, and responses were not varied.

Most of the respondents were interested in the firm's IS and they were aware of the various cyber security risks and threats. Most of the respondents shared this view as indicated by a 4.02 means response, with a low standard deviation of 0.809. The buy-in of individuals in a firm is important in the IS context. Where employees are interested in the security of client information, they may be more receptive of information meant to create awareness regarding the same and readier to comply with requirements in the same context.

A huge number of respondents in the study were also aware that client information should always be kept confidential (mean = 4.89; SD = 0.445). Most of the respondents thus understood the importance of ensuring that client information is kept confidential, which necessitates optimisation of IS within their respective audit firms. This understanding may inform the behaviours of those involved and therefore aid firms' efforts to ensure IS. Conversely, lack of such understanding may see individuals engaging in reckless behaviour thereby exposing firms to serious risk of IS breaches.

Many respondents found discussing audit matters when out with friends or using public transport problematic. This is evidenced by a mean of 1.39, with 0.86 standard deviation recorded. This indicates that most of the respondents disagreed with the researcher on this aspect. Client information can also be effectively exposed if audit company employees purposefully or inadvertently disclose it to third parties.

Furthermore, most of the respondents held the view that client information should never be shared with anyone who is not part of that particular task. The related proposition as put forward by the researcher elicited a mean response of 4.45, with a 0.926 standard deviation. Most respondents thus reckoned that the most ideal situation is one where tasks mimic closed loops within firms with all the relevant client information circulating within the loops made up of those directly involved in a given task. Divulging of such information to any other party even within an organisation would be viewed as a breach of a kind. Lastly, most of the respondents disagreed that pop up messages whilst online are good as one would not miss specials. Most of the respondents reckoned that such pop ups were not good in the context of IS in audit firms. The means response of 1.60 indicated disagreement and the 0.855 standard deviation indicated low variability of responses and high mean reliability. Pop up notification have seen wide use in cyber-attacks with perpetrators employing these in their quest to steal information or gain control over a certain kind of information. However, these are only useful to perpetrators if would-be victims act in a certain way thereby allowing these pop-up notifications to show and open on their devices.

Overall, findings thus show that there were high levels of awareness of client IS threats and interest in the IS aspect of the audit firms.

16 Relevance and Effectiveness of Measures or Strategies Being Utilised in Audit Firms to Safeguard Electronically Stored and Transmitted Client Data

The study also considered the relevance and effectiveness of client IS measures applied by audit firms to safeguard client data. Statements were also put forward by the researcher and respondents had to indicate the extent to which they agreed or disagreed on a 5-point Likert scale. Results are shown in Table 5 below.

Findings in the table above show that there are measures utilised in the firm to safeguard electronically stored and transmitted client data to effectively prevent access, disruption, and modification of information by unauthorised users. The mean response of 4.42 is evidence of this and the standard deviation is 0.616, indicating low variability of the responses provided and high mean reliability. Thus, respondents held the view that their respective audit firms had certain measures in place to ensure client IS. In this context, the assessment of the effectiveness and relevance of IS mechanisms was primarily undertaken logically as opposed to

Table 5 Effective of measures

	Responses	Minimum	Maximum	Mean	Std. deviation
There are measures utilised in the firm to safeguard electronically stored and transmitted client data to effectively prevent access, disruption and modification of information by unauthorised users.	149	3	5	4.42	.616
There are frequent security awareness presentations within the firm that are non-technical and easy to understand.	149	1	5	3.83	1.093
It is okay to send clients information using public email addresses (Gmail, yahoo, etc.).	149	1	5	1.40	.718
All security awareness sessions are mandatory to attend.	149	1	5	3.97	1.033
Access to client information is restricted to only members of that particular audit team.	149	1	5	4.46	.834
Organisational policies on cybersecurity controls are clearly documented and easy to understand.	149	1	5	3.98	.896
Measures utilised in the firm to safeguard electronically stored data are effective in serving their purpose.	149	1	5	4.19	.774
Valid N (listwise)	149				

Source: Primary data

use of any precise metric or actual measure of hardware and software components. The study therefore relied on perceptual responses which reflected the perception of the individuals included in the study regarding the relevance and effectiveness of the measures that are in place. As a result, the perspectives of people working in audit companies provide a clear understanding of the effectiveness and relevance of the measures in place.

Most respondents indicated that there were frequent security awareness presentations within their firms that are non-technical and easy to understand (mean = 3.83; SD = 1.093). Facilitating and making security awareness presentations may not be enough if these are not easily understood by the intended audience. In the current context, audit firms are shown to have mostly undertaken presentations which are easy for the audience to understand. These approaches acknowledge the value of human resources in data security. This signals a shift from the traditional focus areas which saw human resources being largely side lined in this regard.

Many organisations have become aware of the prospect of attacks emerging from inside the entity, leading a significant growth in the relevance of human resource security in the IS environment. The researcher included a statement regarding transmission of client information via personal third-party email services. Most of the respondents disagreed with the researcher regarding the appropriateness of this. The mean response was 1.40 and the standard deviation was low, namely at 0.718. Thus, most of the respondents deemed it not okay to send client information using public email addresses hosted by third parties. These emails may not be the most secure as the influence of the firm on the security of these is limited.

All security awareness sessions run by audit firms are mandatory to attend, and this is the view shared by most of the respondents, as indicated by a 3.97 mean. The standard deviation of 1.033 recorded was low. Employees in most of the firms thus may not have the right to choose whether they want to be part of security awareness sessions or not, as these are mandatory. The importance of IS in audit companies may have influenced their choice.

Moreover, most of the respondents indicated that access to client information is restricted to members of that particular audit team. The mean response recorded was 4.46, with a 0.834 standard deviation. Just like with task teams, client data is shown to have been secured through effective access control to ensure that only audit team members had access to relevant client data.

Most of the respondents also shared the view that organisational policies on cyber security controls are clearly documented and easy to understand. This is shown by a 3.98 mean response, which is a reliable score as indicated by a low standard deviation of 0.896. Thus, most respondents perceived that firms had well documented and understandable cyber security policies.

Findings indicate that measures that are utilised by firms in safeguarding electronically stored data are effective in relation to their purpose. The mean response in this regard was 4.19 and the standard deviation was 0.774. Respondents thus held the view that their audit firms had effective measures in place to ensure the security of client data. This is important for IS. Failure to put in place effective IS measures exposes firms to data breaches which may have a negative effect on firms and their

reputations in the market especially given the firm's duty of care. The importance of effectively safeguarding client information cannot be overemphasised and it has been noted widely in extant literature.

17 Measures Implemented in Small to Medium Audit Firms against Widely Accepted Industry Standards and Frameworks

This was the last objective of the study and it relates to how measures implemented by South African audit firms compare to best practices globally. In order to address the objective, the researcher put forward different best practices in IS and respondents were required to indicate the extent to which they agreed with the assertions by the researcher. Results are shown in Table 6: below.

Most of the respondents agreed with the researcher on the use of hard drive encryption as a measure for securing client information in the firms under study (Mean = 3.94; SD = 0.864). The low mean response score indicates high reliability of the mean score and low variability of the responses. However, respondents were largely uncertain regarding the use of USB port locking, and this is indicated by a mean score of 2.84 that was obtained for the item. Thus, most of the participants were not certain on whether audit firms under study have used USB port locking as an IS measure or not. A low standard deviation of 0.922 was evidence of high reliability of the mean and low variability of responses.

Regarding memory stick encryption, most of the respondents agreed that was the case in their audit firm. The mean response in this regard was 4.02, with a 0.788

Table 6 Measures implemented

	Responses	Minimum	Maximum	Mean	Std. deviation
Hard drive encryption	149	1	5	3.94	.864
USB port locking	149	1	5	2.84	.922
Memory stick encryption	149	1	5	4.02	.788
Use secure remote access methods (e.g. VPN)	149	3	5	4.89	.667
Utilise role-based access controls	149	1	5	4.39	1.022
Internal firewall	149	1	5	4.45	.694
Use of strong passwords	149	2	5	4.60	.758
Involving partners/executives in cybersecurity initiatives	149	1	5	3.94	.982
Utilise intrusion detection systems (IDS)	149	2	5	4.06	1.002
Security awareness sessions conducted frequently	149	1	5	4.08	.746

Source: Primary data

standard deviation. Most of the respondents were of the view that their audit firms had memory stick encryption in place. Findings also show that most of the respondents perceived their firms as utilising secure remote access methods like Virtual Private Network (VPN) in IS (Mean = 4.89; SD = 0.667). Remote access methods were thus perceived to be in use in most of the audit firms that were under study by respondents.

Furthermore, respondents indicated that role-based access control was in place in their audit firm. The results are evidenced by a 4.39 mean score and a standard deviation of 1.022. This suggests that most of the respondents submitted that they worked in audit firms where one's role is an important consideration in determining the kind of access they are given to information. Internal firewalls are also perceived by most of the respondents to be utilised by their audit firms. The mean score was 4.45 while the standard deviation was 0.694. Firewalls are a common information security feature in modern organisations and as observed in the current context, audit firms also utilised these.

This is also the case with the use of strong passwords, which is clearly common amongst audit firms based on the perceptual data drawn from respondents as evidenced by responses from a mean score of 4.60 (SD = 0.758) as recorded. The use of strong passwords can be implemented through ensuring that every member that accesses information has to log in with their password, which is required to be constituted of a certain number or type of characters. Moreover, most of the respondents stated that involvement of partner/executives in cyber security initiatives is a practice that is in place in their respective audit firms. The mean response in this regard was 3.94 while the standard deviation was 0.982. Whilst there may be many facets to how this enhances IS, the most basic way is through ensuring that the necessary management support and buy-in is obtained for these initiatives. This involvement of senior management as well as their support for IS efforts is a widely accepted trend in modern businesses.

Intrusion detection systems are also shown by participants to have been applied in their respective audit firms (Mean = 4.06; SD = 1.002). These relate to a timely detection of any intrusion in the information infrastructure by unauthorised individuals as well as abuse of privileges. This is important in ensuring that the necessary responses are effected in a timely manner to prevent or minimise the damage of such breaches. Lastly, most of the respondents agreed that their audit firms conducted frequent security awareness sessions (Mean = 4.08; SD = 0.746). These are normally administered with a view to ensuring that individuals in a firm have a clear understanding of certain important IS aspects including pitfalls, risk factors as well as best practices. The foregoing takes cognisance of the role of employees, including their attitudes and behaviour in contributing to IS breaches and threats. Creating such awareness amongst employees would circumvent the potential impact of ignorance, and neglect, both of which may have detrimental effects on firms' IS. Efforts to create awareness may prove to be the master stroke as they are likely to also mould the attitude of employees in a manner that may serve to optimise IS.

Suffice to say the findings indicate that respondents perceive that there is a wide application of self-protection measures in an attempt to optimise IS in audit firms.

Self-protection is at the core of IS and it relates to measures that are implemented to protect organisations from IS threats. Self-protection makes use of measures like passwords, firewalls, and intrusion detection systems (IDSs).

18 Level of Awareness among Small to Medium Audit Firms' Trainees and Auditors in Respect of Cyber Related Risk to Confidential Client Information

The above was the first stated objective of the study and results showed that there was generally a high level of awareness amongst the different respondents included in the study. Important IS aspects like the ISP in place within firms, different forms of cyber-attacks and actions that may expose firms to such attacks were well understood by the respondents. The high awareness levels may be a culmination of different aspects, including efforts that firms may have made to ensure that insiders are fully aware of IS matters. In the same vein, there was generally interest in IS matters of the firms in which respondents served, which is direct benefit of the firms' investments.

19 Relevance and Effectiveness of Measures or Strategies Being Utilised in Audit Firms to Safeguard Electronically Stored and Transmitted Client Data

The study also considered the relevance and effectiveness of client IS measures applied by audit firms to safeguard client data. Findings indicated that most firms have implemented measures to safeguard client data that they have electronically stored. These measures have been shown to prevent any form of attacks or breaches of the data which may compromise the integrity, availability, and accuracy of the data. One of the common measures raised was awareness programmes. This shown to be well suited for the audience as they were understandable. Audit firms have also made awareness programmes compulsory, and these have been augmented by well documented IS policies.

20 Measures Implemented in Small to Medium Audit Firms against Widely Accepted Industry Standards and Frameworks

This was the last objective of the study and it relates to how measures implemented by audit firms compared to best practices globally. Results showed that most of the best practices utilised globally have been adopted in the audit firms under study.

Secure access methods, like use of VPNs, are a widely adopted measure amongst firms. The same can be said in the case of role-based access control, which has one's role as the main determinant of the kind of data that they can access. Internal firewall usage has also seen wide use in the audit firms studied with 89.86% responding in the affirmative to questions relating to whether internal firewalls are utilised in their firms. Firewalls are a common IS feature in modern organisations and as observed in the current context, audit firms also utilised these. USB port locking has however not seen much use as only a few firms have been shown to have this measure in place. Hard drive and memory stick encryption have also been fairly utilised in the firms as well as the utilisation of strong passwords. Involvement of partner/executives in cyber security initiatives is a practice that is in place in their respective audit firms.

The measures above are widely applied in IS and in most cases, they are applied in such a way that they complement each other. The use of multiple measures enables a comprehensive approach to protecting information.

21 Recommendations

The study recommends the following:

- Regulators and policy makers should try to provide the necessary guidance with regards to client IS optimisation amongst audit firms. This would help standardise this aspect while also encouraging the adoption of best practices.
- Results showed high levels of awareness regarding cyber related risks to confidential client information that they handle or transmit during and after audit engagements. It is important for management in audit firms to adopt more sustainable approaches to ensure that the high levels of awareness are maintained going forward.
- There is also need for management in audit firms to review measures in place to address cybersecurity risks from time to time given the dynamism and evolution of cybersecurity threats posed by insiders. The regular reviews would help ensure that the measures remain relevant in their usage area.
- Management in audit firms also needs to explore other measures that can be applied in addressing insider threats to IS in an audit environment and this will allow firms to achieve multi-layered security infrastructure while also having in place the most effective measures.
- While results showed a wide adoption and use of global best practices, there is still no universal adoption and management in audit firms should strive to adopt such measures to ensure that is optimised.

References

Aytes, K., & Connolly, T. (2003). A research model for investigating human behaviour related to computer security. *Proceedings of the Americas Conference on Information Systems, 2003*, 2028–2029.

Bogdan, R. C., & Biklen, S. K. (2003). *Qualitative research of education: An introductive to theories and methods* (4th ed.). Allyn and Bacon.

Brodin, M. A. (2019). Framework for GDPR compliance for small- and medium-sized enterprises. *European Journal for Security Research, 4*, 243–264. https://doi.org/10.1007/s41125-019-00042-z

Canongia, C., & Mandarino, R. (2014). Cybersecurity: The new challenge of the information society. In *Crisis management: Concepts, methodologies, tools and applications* (pp. 60–80). IGI Global. https://doi.org/10.4018/978-1-4666-4707-7.ch003

Cheng, C., Flasher, R., & Higgins, J. P. (2019). Accounting firm data breaches: One state's records. *Journal of Accountancy, 227*(6), 1–11. Retrieved November 27, 2021, from http://search.ebscohost.com/login.aspx?direct=true&db=ent&AN=136855027&site=edslive&scope=site

Churchill, G. A., & Lacobucci, D. (2005). *Marketing research: Methodological foundations* (9th ed., p. 697). Thomson.

Cooper, B., Chen, K., Feist, Z., & Kapelke, C. (2017). *The cybersecurity of Olympics sports: New opportunities, new risks*. Center for Long-Term Cybersecurity.

Dunn, C. M., & Egloff, F. (2016). The politics of cybersecurity: Balancing different roles of the state. *St Antony's International Review, 15*, 37–57.

Fagerström, A. (2013). Creating, maintaining and managing an information security culture. Bachelor's thesis. Arcada University of Applied Sciences. Degree Programme in Information and Media Technology.

Hovav, A., & Gray, P. (2014). The ripple effect of an information security breach event: A stakeholder analysis. *Communications of the Association for Information Systems, 34*(1), 50. Retrieved November 27, 2021, from http://search.ebscohost.com/login.aspx?direct=true&db=ent&AN=136855027&site=edslive&scope=site

Hurwitz, R. (2020). The play of states: Norms and security in cyberspace. *American Foreign Policy Interests, 36*(5).

Jemal, A. (2014). User preference of cyber security awareness delivery methods. Behaviour and Information Technology. https://doi.org/10.1080/0144929X.2012.708787

Johnson, E. C. (2016). Security awareness: Switch to a better programme. *Network Security, 2016*(2), 15–18.

Kabanda, G. (2018). A cybersecurity culture framework and its impact on Zimbabwean organizations. Retrieved May 4, 2021, from http://www.academia.edu/download/60361766/Gabriel_Paper_AJMECS_Cybersecurity_Culture_Framework20190822-109031-t3ubm9.pdf

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2018). *What is the impact of successful cyberattacks on target firms? (No. w24409)*. National Bureau of Economic Research.

Khan, F. (2019). Understanding the impact of technology in audit and finance. [Online] Available from https://www.icaew.com/technical/technology

Mugenda, O. M., & Mugenda, A. G. (2003). *Research methods*. Quantitative and Qualitative Approaches.

Mwangi, M. (2017). Financial literacy and financial wellbeing of public sector employees: A critical literature review. *European Scientific Journal, ESJ, 13*(16), 233. NBC News, 15 October 2021).

Peters, G., Shevchenko, P., Cohen, R., & Maurice, D. (2017). Understanding cyber risk and cyber insurance. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3065635.

Ponemon Institute. (2017). *Third annual study on exchanging cyber threat intelligence: There has to be a better way*. Retrieved January 14, 2023, from https://www.ponemon.org/local/upload/file/2017%20Inflobox%20Report%20V6.pdf

PricewaterhouseCoopers. (2021). The Global state of Information security survey 2018. [online]. Available on https://www.pwc.ru/en/publications/global-information-security-survey-2021.html

Public Safety Canada. (2014). Retrieved December 13, 2021, from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dprtmntl-prfrmnc-rprt-2013-14/dprtmntl-prfrmnc-rprt-2013-14-en.pdf

Ramirez, R. B. (2017). Making cybersecurity interdisciplinary: Recommendations for a novel curriculum and terminology harmonization. Thesis, Master of Science in Technology and Policy, MIT.

Rosati, P., Deeney, P., Cummins, M., Van der Werff, L., & Lynn, T. (2019). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in International Business and Finance, 47*, 458–469.

Rosati, P., Deeney, P., Gogolin, F., Cummins, M., Van der Werff, L., & Lynn, T. (2017). The effect of data breach announcements beyond the stock Price: Empirical evidence on market activity. *International Review of Financial Analysis, 49*, 146–154.

Ryan, M. C. (2018). *International cyber conflict and national security*. Oxford handbooks Online: n. pag. Web.

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. *IJARCCE, 7*, 125–128. https://doi.org/10.17148/IJARCCE.2018.71127

Singh, A. N. (2013). Information security management (ISM) practices: Lessons from select cases from India and Germany. *Global Journal of Flexible Systems Management, 14*(4), 225–239.

Solms, R. (2021). Cybersecurity culture: An ill-defined problem. 98–109. https://doi.org/10.1007/9783-319-58553-6_9.

South African Banking Risk Information Centre (SABRIC). (2021). SABRIC releases annual crime stats for 2021. http://www.securitysa.com/17717r

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security, 58*, 216–229. https://doi.org/10.1016/j.cose.2015.12.006

Teddlie, C., & Tashakkori, A. (2004). *SAGE handbook of mixed methods in social and behavioral research* (2nd ed.). Sage.

The Audit Analytics Cyber Security Reports. (2020). https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_EN.pdf

Upton, D. M., & Creese, S. (2014). *The danger from within*. Retrieved January 5, 2023, from https://hbr.org/2014/09/the-danger-from-within.

Woiceshyn, J., & Daellenbach, U. (2018). Evaluating inductive vs deductive research in management studies: Implications for authors, editors, and reviewers. *Qualitative Research in Organizations and Management, 13*(2), 183–195. https://doi.org/10.1108/QROM-06-2017-1538