MARKETING THE IMPACT OF CYBER-ATTACKS ON AN ORGANISATION'S REPUTATION

[1]Visvanathan Naicker; [2]Vhonani Mudau

[1] Cape Peninsula University of Technology
[2]UNISA Graduate School of Business Leadership
Email: [1]naickervi@cput.ac.za; [2]vhonanim1@gmail.com

Received: January 20, 2020; Revised: June 1, 2020; Accepted: December 25, 2020; Published: July 30, 2021

ABSTRACT

Purpose: The rate of cyber-attacks in South Africa has increased in the past five years. Organisations that are operating in a cyberspace have the potential of becoming victims of cyber-attacks, as no organisation is immune to cyber-attacks and related risks.
Design/methodology/approach: This research study adopted a qualitative case study research design. Information was gathered by means of a semi-structured interviews. Thirteen out of the 15 respondents availed themselves for the interviews.
Findings: The study revealed that the role of top management in mitigating the impact of cyber-attacks has not been determined.
Research limitations/implications: The findings of this study cannot be generalised to all public-sector organisations due to their different mandates and objectives, different ways of working, different internal controls and different strengths and weakness. However, other organisations can draw inferences from the implication and outcome of this study.
Practical implications: Cybersecurity matters were not discussed in important forums such as the leadership forum.
Originality/value: Scant research has been conducted in this focus area especially where it involves state owned enterprises. It cannot be assumed, that RAF being a subsidiary entity of the state would have all the required data security and other securities in place to avoid any breach of data theft.

Key Words: cyber-attacks; mitigation; management; risks; security

Paper type: Research paper

1. Introduction

Many organisations store sensitive information that requires adequate protection. Organisations will certainly be in possession of delicate information pertaining to their staff, budget, financial reports and business strategies. Large companies have sophisticated IT and security departments to formulate IT policies, and trained experts for active monitoring of its networks for data breaches. IT departments in large companies are equipped with technical tools to manage internal network security, and they are also likely to procure expensive memberships in public-private partnerships such as information-sharing and analysis centres (ISACs) to obtain high-quality, third-party analysis and intelligence on potential threats (Chak, 2015).

Although information system enables the business by automation of process and ensures that the information is available in real time, etc., the organisation is still prone to

cyber-attacks. When these attacks occur, information is compromised and misappropriated by hackers attempting to manipulate the system by gaining unauthorised access to the organisation's network, or by hacktivists wishing to attack an organisation for political reasons or to manipulate the information system. Another cyber risk is posed by the organisation's own employees who either intentionally or unintentionally abuse their access rights to gain unauthorised access to critical and sensitive organisation information.

2. Background

This study addresses the role of top management in mitigating the impact of cyber-attacks on an organisation's reputation. The study was conducted in one of the state-owned enterprises, namely the Road Accident Fund (RAF) in South Africa. The Road Accident Fund provides a social security safety net to the country and economy by making available compulsory social insurance cover to all users of South African roads.

The RAF provides compulsory cover to all users of South African roads, i.e. citizens and foreigners, against injuries sustained or death arising from accidents involving motor vehicles within the borders of South Africa. This cover is in the form of indemnity insurance to persons who cause the accident, as well as personal injury and death insurance to victims of motor vehicle accidents and their families.
The nature of business or the core operations of the RAF by default expose the Fund to possible fraud and information theft due to the magnitude of data that is collected from the claimants and the confidentiality of the information that is processed within RAF systems.

Management, employees, and the public at large in South Africa still have the perception that cyber-attacks only occur in well-developed countries such as the United States of America, the United Kingdom, and China, among others. However, the latest cyber-attacks that occurred from 2016 until early 2018 revealed that South Africa (including the public and private sector) is prone to cyber-attacks that severely affect the reputation of the organisation. The 2015 Security Summit that was held in Johannesburg from 26 to 28 May revealed that South Africa had suffered from the most cyber-attacks in Africa. The attacks transpire when multiple compromised systems, usually infected with a Trojan, are used to target a single system, causing the websites to be interrupted (Mkhize, 2016). It has been reported that South Africa lost approximately ZAR50 billion in 2014 due to cyber incidents, and that over half a billion online personal records were lost or accessed illegally in South Africa during 2015 (Van Niekerk, 2017). According to the South African Banking Risk Information Centre (SABRIC), South Africa has the third highest number of cybercrime victims worldwide, losing about R2.2 billion a year to cyber-attacks (Iol.co.za, 2018). Although numerous methods and publications on how organisations can manage information security risks are available, many organisations – including small to medium enterprises (SMEs) – still face serious challenges in managing cybercrime and the resulting losses (Bougaardt & Kyobe, 2011).

Executive management in organisations still do not grasp the impact of cyber-attacks, as cyber related topics are not included as a standing agenda during their board meetings where the vision, mission and strategy of the organisation are being discussed. The lack of appetite to manage cyber-attacks extends to the length where the executives and the board do not know which information assets are critical to the organisation, and which measures should be put in place to address related risks. As a result, cyber related risks are not being prioritised, resulting in the organisation's operations being compromised.

2.1 Theoretical background

2.2 Cyber risk management

According to the Institute of Directors in Southern Africa (2016, p. 62), "*the governing body should exercise ongoing oversight of technology and information management and, in particular, oversee that it results in the integration of technology and information risks into organisation-wide risk management*".

Similarly, Dutta and McCrohan (2002) state that corporate boards should ensure that senior managers buy into the process of risk management, as failure to exercise due diligence in information assurance, computer network defence and security in general, exposes the organisation to liability and litigation risk in the event of loss of data, services, or privacy. In addition, risk must be made visible to senior management; that is, executives must play a key role in either accepting those risks or directing activities and enabling resources to mitigate them to acceptable levels from a business, legal, legislative and regulatory standpoint. This requires senior management to have visibility regarding responsibility and accountability in each instance (CGI Group, 2016). There must be disclosure at board level of risks that have the potential to hinder the achievement of business objectives. The disclosure should include strategies to be deployed to mitigate such risks from materialising.

According to Bissell (2013), it is useful for an organisation to understand and agree to the company risk tolerance. Similarly, Dutta and McCrohan (2002) argue that a company needs to determine its acceptable level of risk. In addition, organisations must be aware of their risk tolerance threshold, or level of acceptable risk (CGI Group, 2016). It is therefore very important for organisations to consider defining the risk tolerance or acceptable level of risk that organisation might be faced with in all critical business process. This will outline the acceptable level of risk that an organisation is willing to face in case of cyber-attacks, whether it be damage to the organisation's reputation, loss of revenue, or loss of customer trust, among others

2.3 Reputation damage of cyber-attacks

Cybercrime involves the selling of personal identifiable information such as financial information to other criminal organisations, terrorists, and even to governments. It involves espionage activities where individual proprietary information is sold off for the theft of money from individuals and institutions. Hacktivism is where individuals who are known as hackers use their skills to support a particular ideology. Hacktivist methods include overloading of email servers, website defacement, and denial of service attacks such as social engineering. Insider attacks, on the other hand is when employees share the sensitive information with outsiders to gain some financial benefits or to cause the organisation to make a loss (Yadav & Gour, 2014)

The full consequences of a cyber-incident may take time to surface, which means than the duration of a breach has the potential of affecting some of the organisation's most valued assets, namely its brand and reputation. A growing number of cyber incidents in an organisation are designed with the intention of causing significant operational disruption or damage to a company's market position and/or reputation (Mossburg, 2015; Bissell, 2013; Andrijcic & Horowitz, 2006).

Operational destruction and organisational disruption may be significantly more impactful than data theft alone (Mossburg, 2015). Information security breaches have the

potential of incurring serious losses for organisations, and these losses can be either tangible, such as the loss of business and the maintenance cost of system failure, and/or intangible, such as the loss in customer trust, and loss of the organisation's reputation and competitiveness (Gao & Zhong, 2015).

Moreover, when a company faces a cyberattack, it decreases the trust and faith among its stakeholders, and these people become afraid to invest further in the organisation (Yadav & Gour, 2014). With these kind of attacks, the loss of the company's reputation is a huge downfall for a running business. It is evident that large firms with critical information contained in their database are being breached.

An example of such as breach was during Christmas Eve of 2010, hackers attempted to steal R150 million ($9 million) from the South African Land Bank. The hackers colluded with an internal Land Bank employee and hacked the Land Bank IT system in order to obtain the password to access the bank system. The suspicious transfer of funds was detected by ABSA, who then assisted to prevent the theft in its initial stage. Although the hackers managed to get away with R400 000, Land Bank management had to recover their money.

Similarly, in 2012, a hacker stole R42 million ($2.5 million) from the South African Post Bank. A Post Bank employee used the computer that is linked to the Post Bank main server of a colleague who was on Christmas holiday to transfer money. The money was withdrawn from different banks in South Africa (Van Niekerk, 2017). In October 2017, the personal data of millions of South Africans was compromised when a 27.2 GB database backup file titled "masterdeeds.sql" was leaked publicly online. The data contained millions of ID numbers, as well as contact details, addresses and income of certain individuals.

In 2015, the Al Jazeera's news agency obtained leaked cables from the South African State Security Agency from 2006 to 2014. They published selected excerpts that revealed a number of security flaws and lapses within the South African government and intelligence services. The documents were leaked by an intelligence agent who allowed his brother-in-law to access his official computer.

Although South Africa is a growing nation that has appropriate infrastructure and technology, operation in a cyberspace has exposed the country to numerous successful cyber-attacks which, to a certain extent, has damaged the reputation of the organisations. The majority of the organisations that had been victims to cyber-attacks had severe impacts such as reputational damage.

2.4 Top management’s role and the mitigation of cyber-attacks

For over a decade, there has been a growing need for organisations to understand what cyber security and cyber-attacks are, and how organisations should conduct themselves when operating in cyberspace (Durbin, 2017). The relationship between top management's role to mitigate cyber related risks and the impact on an organisation's reputation as a result of cyber-attacks will focus on the following: Accountability of breach, protection of information as an asset, financial impact of cyber-attacks on an organisation, building cyber resilience to protect the organisation's reputation, impact of security on customers, and the inclusion of information security in the board's agenda.

2.5 Accountability of breach

Due to the transformation of business and where it operates, it has become increasingly clear that in the event of a breach, the hacked organisation will be blamed and held accountable. But this does not spare any senior executives' member and the board from taking accountability of the breach. It is the responsibility of the board and senior executives to be accountable for the breach that occurred. Again, Bonime-Blanc (2017) argues that a massive breach is not an individual error or a technology failure, but rather an organisational breakdown that is the responsibility of top management. Therefore, top management, i.e. the board and senior executives, are ultimately responsible for the breach that occurred, meaning that they must provide guidance in terms of how the organisation should respond to such an attack.

2.6 Protection of information as an asset

CFOs must maintain a thorough understanding of where the vital information is, who might want to steal it, and how they might gain access to it (Durbin, 2017). Similarly, since information is regarded as an asset in the organisation, it is vital for organisations to provide adequate protection to avoid data breaches (IT Governance Institute, 2006), . Protection of information should be a priority for top management. This includes the identification of critical information, the systems and technology where such information is stored, users who have access to such information, and that information is protected and backed up for future retrieval when required.

2.7 Financial impact of cyber-attacks on an organisation

The lack of appreciation and acknowledgement of cyber risk by senior executives is partly because the financial exposure is often not quantified (Gregg, 2010). Dutta and McCrohan (2002) argues that one of the obstacles in engaging senior executives to address information security is the difficulty of connecting security expenditure to profitability. Therefore, an understanding of the potential financial impact of an attack has the potential of helping organisations calibrate their levels of investment (DeHaas & Powers, 2016). It is the responsibility of the board to understand management's rationale for investing in and allocating resources to monitor cyber risk, and building resilience to guard against cyber-attacks, and efforts to expedite response and recovery.

2.8 Building cyber resilience to protect the organisation's reputation

According to the consumer surveys, an organisation that is transparent about cyber security protection is increasingly a determinant in customer loyalty and purchase decisions. In the eyes of regulators and consumers, credibility is bolstered by evidence of comprehensive, ongoing cyber security efforts. In other words, communication with consumers about measures that an organisation has put in place to build resilience against cyber-attacks has the potential of protecting the reputation of an organisation (Durbin, 2017). In addition, according to Ponemon Institute (2018), recognition among top management about how enterprise risks affect their organisation's ability to withstand cyber-attacks has increased from 47% to 57%. Top management is also more aware that cyber resilience affects revenues, brand and reputation. Therefore, it is very important for organisations to communicate the measures that have been taken to build cyber resilience. The communication provides assurance to stakeholders such as consumers, investors and regulators that the organisation will be able to proactively respond to cyber-attacks.

2.9 Impact of security on customers

Top management believes that cyber security is a significant business issue that dramatically impacts the entire organisation's relationship with its customers, profitability, and reputation (Lanz, 2014). Dutta and McCrohan (2002) argues that increases in security have intangible benefits such as customer confidence and goodwill, which are difficult to measure. Therefore, it is critical for top management to realise the need to implement cyber security strategies to guard against cyber-attacks, as this holds unmeasurable and intangible benefits such as customer loyalty, goodwill, increased profitability and the protection of the organisation's reputation.

2.10 Inclusion of information security in the board's agenda

According to IT Governance Institute (2006), information security must be placed on the board's agenda. Similarly, McLean (2013) argues that because the responsibility to manage cyber risks rests with each organisation, it needs to be high on each board's agenda. In addition, according to the findings of PWC's 2014 Investor Survey, the results showed that 84% of investors believe the company board should discuss cyber security issues, but only 57% of boards of directors were reported to have had discussions on cyber security issues in their board meetings (Balbi, 2015). On the other hand, Bonime-Blanc (2017) argues that there must be a structured top-down approach that embeds cybersecurity management through the company infrastructure. The best approach is to establish a dedicated technology committee on the board with a mandate that includes the responsibility to review cybersecurity and ensure that discussions of this risk and opportunity are reported to the board.

Contrary to this, Werlinger, Hawkey, and Beznosov (2008) argue that organisational factors such as an open academic environment, distribution of IT management, interaction with other organisations, and controlled access to data distributed in different departments increased technical complexity.

Curry (2017) state that while cybersecurity is now on the agenda at board meetings, this does not mean that board members understand how to tackle the cyber security issue, as most of the board members have expertise in other forms of risk, and not in how to protect corporate assets from cyber-attacks. Therefore, although there is a need for inclusion of cyber security risks in the board's agenda, there should be a clear distinction as to whether the board should be primarily responsible to discuss cyber security issues or whether a subcommittee of the board responsible for security should be appointed with a mandate to report to the board on matters discussed on a regular basis. Also, there is a need for benefit realisation in instances where cyber security issues are included in the board's meeting agenda, but board members have limited understanding of cyber security and what should be done to upskill the board.

3. Research methodology

Yin (1994, as cited in Lee,1999) says that the evidence that supports the case study research design can potentially come from six sources, namely documents; archival records, interviews, direct observations, participant observations, and physical artefacts (Leedy & Ormrod, 2015).

In this qualitative research, a case study was used to gain a rich, detailed understanding of the problem by examining the role of top management in mitigating cyber related risks and the impact on the organisation's reputation in detail.

Case studies also emphasise detailed contextual analysis of a limited number of events or conditions and their relationships. Data on the employees' perception of the role of top management in mitigating the impact of cyber-attacks on an organisation's reputation was collected using semi-structured interviews. Both empirical and non-empirical approaches were used.

The three types of data collection methods employed were: the literature reviewed; in depth interviews and information gleaned from the pilot study. The questions were adapted and developed from previously validated questionnaires. The questionnaires were disseminated to the respondents using email prior to the interviews. This ensured a convenient, fast and manageable data collection process (Adams & Cox, 2008).

The population were employees of the ICT business unit within the Road Accident Fund. The sample included employees from different divisions within ICT, viz. ICT Governance, Risk and Security Application Development, Infrastructure Services, and ICT Operations. The sample group interviewed were RAF employees, primarily from the ICT division.

Convenience sampling was used because the respondents were available regarding access, location, time and willingness (Lopez & Whitehead, 2013). Table 1 below depicts the sample size for the study:

Table 1: Sample framework

Operational unit	Total population	Sample size	% of population	Sample method
Information and Communication Technology	139	15	18%	Convenience sampling

A pilot study was conducted on five employees eliminating potential problem areas during the main data collection stage. Validity, reliability and triangulation procedures were conducted.

Table 2 shows the linking of the research objectives to the interview questions.

Table 2: Linking of objectives to questions

Research objective	Interview questions
RO1: To determine whether the impact of cyber-attacks relating to an organisation's reputation (and possible damage to such reputation) has been identified	• What is your understanding of a cyberattack? • What is the possible impact/severity of a cyberattack to an organisation's reputation? • To the best of your knowledge, when was the last time the RAF experienced a cyberattack (if any)? Was there any significant reputational impact for the organisation?

Research objective	Interview questions
RO2: To determine whether management has put controls in place to address cyber-attacks and related risks in the organisation	• In your own opinion, do you believe there are enough controls at the RAF to prevent the occurrence of cyber-attacks? May you please share with me some of the controls? • What measures can the RAF put in place to ensure that employees are aware of the latest patterns that are used to penetrate and attack an organisation? • What impact does continuous training and education around cyber-attacks have on the employees? • What suggestions can you offer to the RAF should cyber-attacks happen in the future?
RO3: To determine whether governance documents to manage cyber-attacks and related risks in the organisation have been developed and approved	• What governance documents, i.e. policies, have been developed and approved specifically to address the issues around cyber-attacks and cyber security?
RO4: To determine whether top management responsibilities have been identified to manage and address cyber-attacks and related risks	• Suppose there is a cyberattack on the organisation, which people within the RAF are responsible for responding to the impact of the attack and why? • In your view, what should the role of top management be in the event of a cyberattack? • In your own opinion, is top management (Executive Committee) aware of the serious threats posed by cyber-attacks? Motivate your answer • Do you believe that top management is doing enough to address cyber related risks? In other words, is top management setting the tone from top to the bottom to address cyber security related risks?
RO5: To confirm whether the topic of cyber related risks and security has been included as a standing agenda item in board of directors meetings	• Does top management discuss cyber security matters at important forums such as board meetings? If so, name the forum in which the cyber security issues are discussed.

In case study research, Yin (2003) discusses the need for searching the data for "patterns" which may explain or identify causal links in the database. Therefore, during the data analysis process, data concepts, themes (themes will be allocated to groups of responses) and meanings were identified in order to evaluate the data and reach a conclusion. This included identification and grouping together similar responses from participants. The chosen method for data analysis was content analysis.

4. Findings and discussions

Thirteen interviews were conducted at the RAF (ICT Business Unit). The interviews were recorded with the full consent of the participants. The recordings were then transcribed verbatim. Ten males and three females were interviewed and were in positions such as senior managers, managers and ICT specialists. The presentation of the findings on demographics has been presented in one graphical representation as depicted in Figure 1 below.

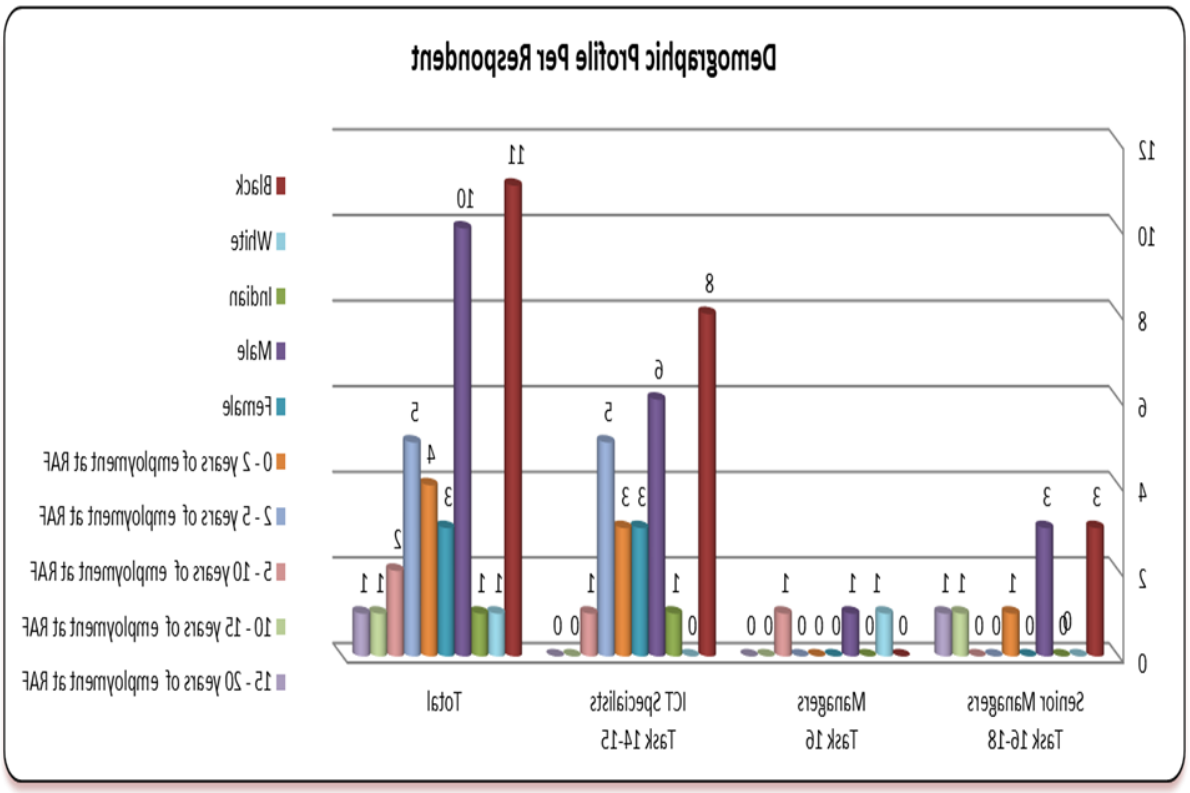

Figure 1: Demographic profile per respondent

The following are the results from the interviews addressing the above stated objectives.

4.1 Findings on the impact of cyber-attacks to an organisation's reputation

The understanding of cyber-attacks by the individuals who participated in the study was twofold: One, the purpose of a cyberattack is to gain unauthorised access through the use of technology. Two, a cyberattack is part of cybercrime where one individual or group of people will try to attack or gain access to organisational infrastructure in order to steal information. Although the respondents had different responses/views relating to the understanding of cyber-attacks, their understanding is in accordance with the description of cyber-attacks. The elements of cyber-attacks that came out in the responses are attacks through cybercrime,

hacktivism and inside threats. Cybercrime involves the selling of personal identifiable information (such as financial information) to other criminal organisations, terrorists, and even governments. It involves espionage activities where individual proprietary information is sold off for the theft of money from individuals and institutions. This is achieved by making use of tools such as malware, identity theft, and cyber warfare, among others (Sheldon, 2012). Hacktivism is where individuals who are known as hackers use their skills to support a particular ideology. Hacktivist methods include overloading of email servers, website defacement, and denial of service attacks such as social engineering. Although they have been known to use worms and viruses, their maliciousness is highly focused against the targeted organisation in order to achieve far-reaching consequences (Meyers, Powers, & Faissol, 2009). Insider attacks occur when an organisation faces a threat from its own employees. The employees share sensitive information with outsiders to gain some financial benefits or to make the organisation suffer some or other form of loss, whether it be financial, reputational or some other significant loss (Yadav & Gour, 2014).

4.2 Impact of cyber-attacks on an organisation's reputation

The damage to the reputation of the organisation was perceived to be the loss of trust resulting in people not being willing to supply their information, seeing that the organisation would have violated the responsibility to secure the personal information received. Furthermore, the organisation will not be able to fulfil its primary mandate, which is to compensate road accident victims. According to Yadav and Gour (2014). when a company faces a cyberattack, it decreases the trust and faith among the people (stakeholders) and people are afraid to invest further in the organisation. In addition, information security breaches have the potential of incurring serious losses for organisations, which can be either tangible such as the loss of business and the maintenance cost of system failure, and/or intangible such as the loss in customer trust, reputation and competitiveness (Gao & Zhong, 2015).

4.3 Previous incidents of cyber-attacks at RAF

The majority of the respondents were not aware of cyberattack related incidents that have occurred at the RAF. This creates the perception that the existing controls have the potential of preventing and detecting the occurrence of cyber-attacks, which is evidenced by the fact that there have not been cyber-attacks and/or major breaches that had damaged the reputation of the organisation. However, this should not give the organisation cause for relaxation and erroneously thinking that it has sufficient controls in place to prevent the occurrence of cyber-attacks, because the attackers invent new ways of attacking the cyberspace every day. According to Van Kessel (2017), organisations may feel more confident about confronting the types of attacks with which they have become familiar in recent years; however, they still lack the capability to deal with more advanced, targeted assaults; they may not even be aware of new attack methods that are emerging.

4.4 Findings on the controls to address cyber-attacks and related risks

Because the RAF is operating in cyberspace, the types of controls that have currently been implemented were regarded as "not enough" to prevent the occurrence of cyber-attacks, as attackers identify new ways of attacking organisations almost every day. Controls that are in place include database activity monitoring tools, identify-and-access management, back-ups, anti-virus protection for end-points and patch management processes, among others. However, technology alone was regarded as insufficient to secure the environment. The alignment between technology, processes and people was identified as an element that requires attention. Dutta and McCrohan (2002) state that while technological solutions are the responsibility of

the IT staff, senior managers must be familiar with some of the critical components of security technology. However, the controls implemented are only technology based, therefore there is a need to align technology, processes and people. According to Gray (2006), a purely techno-centric approach can be misleading. Not only does it leave out people issues, but, because of its fascination with the latest technologies, it can lose sight of the continual changes that affect the way systems perform. In addition, Bissell (2013) states that cyber security is a collective assimilation of an organisation's people, processes and technologies that combine to provide mitigations to cyber security threats. In order for the organisation to be secured against cyber related threats, critical technology and infrastructure must be identified and stringent controls implemented to build resilience against cyber related attacks.

4.5 Awareness of latest patterns used to penetrate and attack the organisation

The need for continuous training and cyber related communications as a form of raising awareness among employees was identified as measures that must be put in place to ensure that employees are aware of the latest patterns that are used to penetrate and attack organisations. The International Telecommunication Union (ITU) defines the creation of a cyber-security culture as the best guarantee for cyber security (International Telecommunication Union, 2008). According to Ghernouti-Hélie (2010), one of the pillars of such a culture is awareness and education. In order to achieve a cyber-security culture, user awareness is the first guideline, meaning users should be well informed about the necessity for cyber security and the steps they can take to promote it. In other words, implementing security awareness programmes and initiatives for users of systems and networks, develop awareness of cyber threats and available solutions to mitigate it. Secondly, users must realise the need for security as a critical element for cyber security and know how to apply the relevant security measures. Therefore, spreading awareness and educating the users of cyberspace is an important element of promoting the cyber security culture. Education and awareness are elements that underpin cyber security as a whole, that is, play a vital role in cyber security (Kortjan, 2013). Moreover, Lindström and Hägerfors (2009) state that the education, practice and awareness should include IT and information security training on the business continuity plan, security polices, and general security training and an awareness programme for all members of an organisation as well as specific security training for senior management.

4.6 Impact of continuous training and education to employees

Continuous training and education of employees around cyber-attacks was regarded as one of the control measures that will make the employee more vigilant and create a safe environment. According to (Kortjan, 2013), a cyber-security workforce that is well equipped with the requisite knowledge, as well as cyber citizens who are well aware of the nature of cyberspace and the risks that come with a lifestyle that is highly interwoven into cyberspace, will create a safe environment, because users are aware and alert when operating in cyberspace. Moreover, continuous training and education of employees around cyber-attacks encourages internet users to practise safety precautions, and trains them in online defence methods. Furthermore, it equips users with cyber security skills on all the aspects of cyber security so that not only the organisational network infrastructures are kept resilient to cyber-attacks and threats, but the users are also well informed (Dlamini, Taute, & Radebe, 2011).

4.7 Findings on governance documents to manage the impact of cyber-attacks

Not one interviewee was aware of any governance documents, i.e. policies that have been developed and approved specifically to address the issues around cyber-attacks and cyber security. The Information Security Policy had elements that address information security;

however, a document that specifically addresses cyber-attacks and cyber security risks had not been developed. A cyber security strategy is considered as a way to identify key societal sectors and subsectors, to assess specifics of these sectors, to identify organisational prerequisites, to assess the threat environment in the area of interest, and to establish a comprehensive coordination and management process (Klaic, 2015). In addition, the efforts to guard against cyber-attacks include the development of a strategy that will govern the manner in which the message of cyber security is communicated to the public (Kortjan, 2013).

4.8 Findings on top management's responsibility towards addressing cyber-attacks

The (ICT) security team was regarded as the people primarily responsible for managing and addressing the issue of cyber-attacks and related risks. The respondents' views portray the general understanding that cyber security and cyber-attacks is an Information Technology (IT) issue. However, Gregg (2010) argues that cyber-attacks are no longer an IT executive issue, as this matter requires an enterprise-wide management approach to quantifying and addressing cyber risks where all executives will look at the larger cost and business issues they pose which may hinder the successful running of the organisation.

4.9 The role of top management in the event of a cyberattack

Although the role of top management was viewed by the majority of the respondents as one of having to ensure that the information is secure and to communicate with everyone, the level of accountability of top management in the event of a cyberattack had not been determined. Therefore, according to Curry (2017), it is the responsibility of the board and senior executives to be accountable for the breach that has occurred. A massive breach is not an individual error or a technological failure; it is an organisational breakdown that is the responsibility of the top management.

4.10 Top management's awareness of serious threats posed by a cyberattack

There were contrasting views in terms of top management's understanding of the serious threats posed by cyber-attacks. The majority of the respondents were of the view that top management is aware of the serious threats posed by cyber-attacks. This can be seen by the investment that is being made in ICT and supported by management. On the other hand, the fact that top management supports the ICT initiatives does not mean that they are aware of the serious threats that are posed by cyber-attacks, as they could be doing so with an understanding that ICT knows that they are doing and support them on that. According to Werlinger, Kirstie and Konstantin (2008), the greater the top management support, the more effective the security within organisations, as organisations spend more resources on preventive measures to avoid security incidents. Moreover, to improve the chances of fighting back against cyber attackers, organisations will have to overcome the barriers currently making it more difficult for cybersecurity operations to add value, one of these barriers being a lack of understanding and awareness among top management employees when it comes to the serious threats posed by cyber-attacks (Van Kessel, 2017).

4.11 Top management setting the tone from top to bottom

The respondents' view was that top management are not setting the tone from top to bottom to address cyber security and related risks. The issues relating to cyber security and related risks are addressed only in messages that come from ICT, and many of the employees might not know where they fit in the cyber risk management process. Respondents believe cyber related risks should be discussed in important forums such a Leadership Forum for management. Moreover, the lack of tone from the top to bottom to address cyber related risks

was regarded as an organisational culture issue wherein only matters pertaining to achieving the RAF Annual Performance Plan are discussed and given much attention/emphasis.

The visible actions taken by senior management in support of the organisation's values are significant to employees. In order to establish what is considered as important within an organisation, employees look for consistent patterns, and watch and listen to those above them. When senior management not only says that something is significant, but also consistently behaves in a manner which supports this statement, employees begin to believe what is said (O`Reilly, 1989). Moreover, Durbin (2017) argued that senior management/executives and the board should consider taking a more active oversight role in promoting an integrated approach to IT strategy and cyber security.

4.12 Findings on top management's discussion of cyber security matters

There were contrasting views in terms of whether top management discusses cyber security related matters at important forums such as board meetings. The majority of the respondents were of the view that they do not know if cyber related risks are included as an agenda item in the board of directors' meetings. On the contrary, very few respondents agreed that top management discussed cyber security matters at important forums such as IT Steering Committee meetings, Operations and Information Technology Committee meetings and board meetings.

However, since there were a few respondents who were of the view that cyber security matters are discussed at important forums such as board meetings, this depicts an organisational culture that lacks top-bottom communication. Werlinger, Kirstie and Konstantin (2008) argue that organisational factors such as an open academic environment, distribution of IT management, interaction with other organisations, and controlled access to data distributed in different departments increased technical complexity.

The inclusion of cyber security matters in the board meeting agenda in future was viewed by respondents as critical, as the board (together with top management) must set the tone from top to bottom regarding the criticality of cyber security and cyber-attacks. Mclean (2013) argues that because the responsibility of managing cyber risks rests with each organisation, it needs to be high on each board's agenda. Moreover, Bonime-Blanc (2017), also argues that there must be a structured top-bottom approach that embeds cybersecurity management through company infrastructure. The best approach is to establish a dedicated technology committee on the board with a mandate that includes the responsibility to review cybersecurity and ensure that discussions of this risk and opportunity are reported to the board

5. Conclusions and recommendations

Objective 1: *To determine whether the impact of cyber-attacks in relation to the organisation's reputation has been identified.*

Based on the responses received, it can be concluded that RAF employees understand the meaning of cyberattack. Moreover, the impact of cyber-attacks relating to an organisation's reputation has been identified as loss of trust, which will result in people not interested in doing business with the RAF; that is, stakeholders will not be willing to provide the personal information required in order for road accident claims to be processed. However, the RAF has not been the victim of any cyberattack that resulted in the reputation of the organisation being affected.

Objective 2: *To determine whether controls have been put in place by management to address the issue of cyber-attacks and related risks in the organisation.*
It was concluded that the existing controls are not enough to prevent the occurrence of cyber-attacks. Control mechanisms that link technology, processes and people were perceived to have the potential of protecting the environment and organisation at large against cyber-attacks. Furthermore, continuous awareness and training of employees was identified as a critical control that has the potential of reducing the occurrence of a cyberattack, as awareness was perceived as an element that creates a safe environment.

Objective 3: *Governance documents, i.e. policies have been developed and approved specifically to address the issues around cyber-attacks and cyber security.*
Although the Information Security policy was perceived to have addressed some of the elements of information security, it was concluded that a document to address the issues around cyber-attacks and cyber security had not been developed; that is, there is a need to develop a cyber-security strategy.

Objective 4: *To determine whether top management's responsibilities have been identified to manage and address cyber-attacks and related risks*
It was concluded that the responsibilities of top management to manage and address cyber-attacks and related risks had not been identified because of the following:

- The ICT Security Team was regarded as the people responsible for responding to the impact of a cyberattack.
- Part of top management's role is to assess the impact of cyber-attacks and communicate this to everyone within the organisation which was found to be a gap.
- Although top management is perceived by the majority of interviewees as being aware of the serious threats posed by cyber-attacks because they support the ICT initiative, it was concluded that this does not mean that they understand the serious threats that the organisation is faced with as a result of cyber-attacks. This is evidenced by the level of trust that the organisation has for ICT department.
- Top management has not set the tone from the top to bottom to address cyber security and related risks, because these matters were discussed only at ICT and not included as an agenda item at important forums such as the Leadership Forum for management.

Objective 5: *To confirm whether the topic of cyber related risks and security has been included as a standing agenda item in board of director's meetings.*
It was concluded that there was no clear view among the employees at large on the matters that are discussed at board meetings. Information was circulated only to affected employees or on a need-to-know basis

The following conclusions can be drawn from the study to address the research questions. The role that top management of RAF needs to play in assessing the impact of cyber-attacks (should they materialise) has not been fully defined. The people primarily responsible for responding to cyberattack incidents were perceived to be the ICT security team, with top management's role being that of assessing the impact of a cyberattack and communicating this to employees within the organisation. Respondents perceived top management as lacking in accountability and guidance in terms of how employees should conduct themselves in instances where cyberattack incidents have occurred.

The organisation has been supporting ICT initiatives that are aimed at building resilience against cyber-attacks and related risks. However, by providing support, it could not be concluded that top management understands the serious threats that are posed by cyber-attacks, as top management appears to believe and trust that their ICT department knows what needs to be implemented and supports them on those initiatives.

Furthermore, top management was not setting the tone from the top to bottom, as cyber security and cyber related risks were only emphasised by ICT; that is, there was no constant message coming from top management emphasising the emergence of cyber related risks and identifying those employees who are expected to manage such risks. This was evident by the lack of discussions around security matters in important management forums such as the Leadership Forum. Moreover, only affected employees knew whether the issue of cyber-attacks and related risks were discussed at important forums such as board meetings, which portrays an organisational culture that is lacking in top-bottom communication.

The RAF has implemented controls to minimise cyberattack incidents. Currently, it can be concluded that the existing controls have the potential of preventing and detecting cyber-attacks and related risks, as there has not been any major exposure that caused the reputation of RAF being damaged as a result of cyber-attacks. However, the controls that exist were not enough to secure the environment from future cyber-attacks and related risks, because attackers invent new ways of attacking organisations every day. Therefore, technology, processes and people need to be aligned in order to achieve an end-to-end secure control environment.

In conclusion, the development of a cyber-security strategy has a potentially of addressing the weaknesses that currently exist in the organisation, as such a strategy would clearly define the roles and responsibilities of every person involved in cyber security, and a task team would be identified and appointed.

6. Recommendations

The RAF should introduce an organisational culture of constant communication from top to bottom. It is important for top management to communicate with their employees. The tone that the board is setting at the top regarding cyber security matters is important, so that employees are informed of what is expected from them and the processes and systems that are critical in order for the organisation to meet its strategic objectives. Top management should show genuine interest and be willing to study how best to engage with the workforce to educate staff and build awareness around the threat posed by a cyberattack. This is often about changing the culture such that employees are alert to the risks that will make the organisation vulnerable to cyberattack challenges (Barlock, Buffomante, & Rica, 2014).

Risk oversight is also a key competence of the board, and disclosure about the board's involvement in the oversight of the risk management process should provide important information to employees about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company (Aguilar, 2016).

Moreover, to ensure visibility of the matters that are of high priority to top management and the board, agenda items for forums at the RAF, i.e. the Leadership Forum should include:

- The discussion of emergence of cyber security risks;

- What is expected from RAF employees;
- The initiatives that have been implemented and/or are to be implemented to ensure end-to-end security of the control environment;
- Whether the organisation is ready to respond to the impact of a cyberattack should it occur; and
- What the organisation intends to do to protect its reputation.

7. References

Adams, A., & Cox, A.L. (2008). Questionnaires, in-depth interviews and focus groups, Research Methods for Human Computer Interaction. *Cambridge University Press,* Cambridge, UK, pp. 17–34.

Aguilar, C.L.A. (2016).The Role of Boards of Directors and CISOs in Overseeing Cyber - Risks: *Security Adviser Alliance Conference*, pp. 1–15.

Andrijcic, E., & Horowitz, B. (2006), A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property. *Risk Analysis, 26*(4), 907-923.

Balbi, A. (2015). Discussing cyber-security at the board level. *Strategic Finance, Montvale, 96*(7), 22–24

Barlock, S., Buffomante, T., & Rica, F. (2014). *Cyber-security: It's not just about technology*, U.S.A, Retrieved from https://assets.kpmg.com/content/dam/kpmg/pdf/2014/05/cyber-security-not-just-technology.pdf.

Bissell, K. (2013). A strategic approach to cyber. *Financial Executive, 29*(2), 36-41.

Bonime-Blanc, A. (2017., *A strategic cyber-roadmap for the board, Harvard Law School Forum on Corporate Governance and Financial Regulation*. Harvard Law School, Retrieved from https://corpgov.law.harvard.edu/2017/01/12/a-strategic-cyber-roadmap-for-the-board/.

Bougaardt, G., & Kyobe, M. (2011). Investigating the Factors Inhibiting SMEs From Recognizing and Measuring Losses from Cyber Crime in South Africa, *The Electronic Journal Information,14*(2), 167–178.

Chak, S.K. (2015), Managing Cybersecurity as a Business Risk for Small and Medium Enterprises, Baltimore.

CGI Group. (2016). IT Security Governance - A holistic approach, CGI Group INC

Curry, S. (2017). Boards Should Take Responsibility for Cybersecurity. Here's How to Do It, Hbr.Org, 16 November, available at: https://hbr.org/2017/11/boards-should-take-responsibility-for-cybersecurity-heres-how-to-do-it.

Dehaas, B.D. and Powers, E. (2016). Sharpening the Board ' s Role in Cyber-Risk Oversight, No. February, available at: https://www2.deloitte.com/us/en/pages/center-for-board-effectiveness/articles/sharpening-the-boards-role-in-cyber-risk-oversight.html.

Dlamini, I. Z., Taute, B., & Radebe, J. (2011). Framework for an African Policy Towards Creating Cyber Security Awareness, Proceedings of Southern African Cyber Security Awareness Workshop (SACSAW) 2011, researchspace.csir.co.za, pp. 15–31.

Dutta, A., & McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review, 45*(1), 67-87.

Durbin, S. (2017), Boards And Cyber Security: Is Your C-Suite Ready?, *The Corporate Board*, *38*(226), 8–12.

Gao, X., & Zhong, W. (2015). Information security investment for competitive firms with hacker behavior and security requirements. *Annals of Operations Research*, *235*(1), 277–300.

Gray, P. (2006), Innovating then and now, Information Systems Management. *Auerbach*, *23*(4), 80–84.

Gregg, B.R. (2010). The CFO's Role in Managing Cyber Risk, Financial Executive, No. september, pp. 61–63.

Ghernouti-Hélie, S. (2010). A National Strategy for an Effective Cybersecurity Approach and Culture, In 2010 International Conference on Availability, Reliability and Security, pp. 370–373.

International Telecommunication Union. (2008), Global Security Report, Retrieved from http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf.

IT Governance Institute. (2006). Information Security Governance : Guidance for Boards of Directors and Executive Management, 2nd Edition. Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/Information-Security-Govenance-for-Board-of-Directors-and-Executive-Management_res_Eng_0510.pdf.

iol.co.za. (2018), South Africans losing R 2.2 billion a year to cyber attacks, Iol.Co.Za, Cape town, 21 June, Retrieved from https://www.iol.co.za/capeargus/news/south-africans-losing-r22-billion-a-year-to-cyber-attacks-15601682. 67–87.

Klaic, A. (2015). A Method for the Development of Cyber Security Strategies Information & Security. *An International Journal*, *34*(1), 37-55.

Kortjan, N. (2013). *Noluxolo+Kortjan*, Nelson Mandela Metropolitan University.

Lanz, J. (2014), Cybersecurity Governance: The Role of the Audit Committee and the CPA. *CPA Journal*, *84*(11), 6–10.

Lee, T. (1999). Using Qualitative Methods in Organisational Research, Thousand Oaks, CA: SAGE,

Leedy, P. D., & Ormrod, J. (2014). Practical Research Planning and Design (Tenth Edition), University of Northern Colorado..

Lopez, V., & Whitehead, D. (2013) Sampling data and data collection in qualitative research. In: Nursing & Midwifery Research: *Methods and Appraisal for Evidence-Based Practice* (4th edn.). (Schneider, Z., & Whitehead, D; LoBiondo-Wood, G., & Haber, J.), Elsevier - Mosby, Marrickville, Sydney. pp. 123-140.

Lindström, J., & Hägerfors, A. (2009). A model for explaining strategic IT-and information security to senior management. *International Journal of Public Information*, *5*(1),17–29.

Mclean, S. (2013), Beware the Botnets : Cyber Security Is a Board Level Issue. *Intellectual Property & Technology Law Journal*, *25*(12), 22–27.

Meyers, D., Powers, S., & Faissol, D. (2009). *Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches.* Lawrence Livermore National Laboratory.

Mkhize, H. (2016). "The 11th Itweb Security Summit", Department of Telecommunications and Postal Services, Retrieved from https://www.dtps.gov.za/index.php?option=com_content&view=article&id=627:speech-by-the-deputy-minister-of-the-department-of-telecommunications-and-postal-services,honourable-prof-hlengiwe-mkhize-during-the-occasion-of-the-11th-itweb-security-summit&catid= (accessed 23 November 2018).

Mossburg, E. (2015). A Deeper Look at the Financial Impact of Cyber Attacks, Retrieved from https://daily.financialexecutives.org/a-deeper-look-at-the-financial-impact-of-

cyber-attacks.
O`Reilly, C. (1989). Corporations, culture and commitment: motivation and social control in organizations. *California Management Review*, *31*, 9–24.
Ponemon Institute. (2018), The Third Annual Study on the Cyber Resilient Organisation, Australia, Retrieved from https://www.ibm.com/downloads/cas/ZD2PL2MK
Sheldon, J. B. (2012), State of the art; attackers and Targets in Cyberspace. *Journal of Military and Strategic Studies*, *12*(2), 1–19.
The institute of directors in Southern Africa. (2016). King IV report on corporate governance for South Africa 2016, The Institute of Directors in Southern Africa 2016, pp. 1–120.
Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication (AJIC), 20*, 113–132.
Van Kessel, P. (2017). *Cybersecurity regained: Preparing to face cyber attacks.* 20th Global Information Security Survey 2017–18, EYGM Limited, pp. 1–32.
Werlinger, R., Hawkey, K., & Beznosov, K. (2008). *Human, organizational and technological challenges of implementing IT security in organizations.* Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISA), No. 2, pp. 1–10.
Yadav, H., & Gour, S. (2014), Cyber Attacks: An impact on Economy to an organization. *International Journal of Information & Computation Technology*, *4*(9), 937–940.
Yin, R. K. (1994), Case Study Research: Design and Methods, Sage. Publications (2nd ed.). Newbury Park, CA: Sage.