A Framework to Implement Information Security Awareness, Education and Training within the Limpopo Economic Development Agency Group

by

Ntsewa Benjamin MOKOBANE

217885993

TREATISE

for the fulfilment of the degree

MPhil in IT Governance

in the

Faculty of Engineering, the Built Environment and Information Technology

of the

Nelson Mandela University

Supervisor: Professor Reinhardt A Botha

April 2019

NELSON MANDELA
UNIVERSITY

DECLARATION BY CANDIDATE

NAME : Ntsewa Benjamin MOKOBANE

STUDENT NUMBER : 217885993

QUALIFICATION : MASTER OF PHILOSOPHY IN INFORMATION TECHNOLOGY GOVERNANCE

TITLE OF PROJECT : A FRAMEWORK TO IMPLEMENT INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING WITHIN THE LIMPOPO ECONOMIC DEVELOPMENT AGENCY GROUP

DECLARATION:

In accordance with Rule G5.6.3, I hereby declare that the above-mentioned treatise/dissertation/thesis is my own work and that it has not previously been submitted for assessment to another University or for another qualification.

Ntsewa Benjamin Mokobane
11 March 2019

ACKNOWLEDGEMENTS

I would like to express my deep gratitude to Professor Reinhardt A. Botha, my research supervisor, for his patient guidance, enthusiastic encouragement and useful critiques of this research work. I would also like to thank Professor Rossouw von Solms, for his advice and assistance in keeping my progress on schedule.

My grateful thanks are also extended to Messrs. Skhumbuzo Khoza, Daniel Maloba, Thulani Mahlangu, Isaac Mamakoa and Ms Unity Mabitsela for the role they played as the Cybersecurity Interest Team.

I would also like to extend my thanks to my brother Eric and his wife Edzani for their help in supporting me between their home and the airport.

Finally, I wish to thank my wife Dora and sons Pitsi and Motubatse for their support and encouragement throughout my time of study.

ABSTRACT

Cybersecurity awareness, education and training of employees is key in reducing and preventing cyber-attack opportunities. The ignorance and/or lack of understanding of employees about the information security risks around them might expose the LEDA Group to cyber-attacks. This led to the problem that the level of awareness of employees regarding information security was not known. The implication of this not knowing was that an argument for the nature of an intervention to ensure awareness, as well as to educate and train employees regarding information security was not possible.

The aim of this treatise was to develop a framework as an effective guideline for the implementation of cybersecurity awareness, education and training of employees.

In the study, the LEDA Group employees were surveyed to determine their cybersecurity knowledge gap. An online questionnaire was randomly sent to 314 LEDA Group employees. The survey was voluntary and confidential. One hundred and thirty seven (137) employees completed the survey. The results of the survey were analysed to determine the gap between the current cybersecurity knowledge of the LEDA Group employees and state-of-the-art cybersecurity knowledge. The gap was used in the development of the framework for the implementation of the cybersecurity awareness, education and training (F-CSAET).

Central to F-CSAET is the governance principles guided by best practices such as King IV, COBIT5, ISO27001, ISO27005, ISO27008 and ISO27032 and the compliance requirements to POPIA, the Copyright Act and the Cybercrimes and Cybersecurity Bill. The F-CSAET has six steps, namely Assess, Analyse, Create, Plan, Implement and Reinforce.

The framework was evaluated for applicability by the team called the cyber security interest team, which was established specifically for the purpose of the F-CSAET.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

ANOVA	One Way Analysis of Variance
CIO	Chief Information Officer
CIT	Cybersecurity Interest Team
CSAET	Cybersecurity awareness, education and training
F-CSAET	Framework for Cybersecurity awareness, education and training
HAIS-Q	Human Aspects of Information Security Questionnaire
Http	Hypertext transfer protocol
Https	Hypertext transfer protocol secure
ICT	Information and Communication Technology
IDP	Individual Development Plan
IoDSA	Institute of Directors SA
IKPM	Information, Knowledge and Projects Management
IoT	Internet of Things
ISACA	Information Systems Audit and Control Association
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
IT	Information Technology
KAB	Knowledge, Attitude and Behaviour
LEDA	Limpopo Economic development Agency
NLP	Neurolinguistic programming
NMU-DSFM	Nelson Mandela University – Design Science Framework Methodology
PII	Personally Identifiable Information
PIN	Personal Identification Number
POPIA	Protection of Personal Information Act
SMS	Short message service
USB	Universal Serial Bus
VPN	Virtual Private Network

CHAPTER 1: INTRODUCTION

In this chapter the basis for this research will be unpacked, as well as what the research aimed to achieve. First, the workplace environment will be looked at where the pervasive use of the Internet, mobile devices and their cybersecurity risks, as well as cyberspace and its characteristics, and cyber risks will be discussed. The impact of no or less cybersecurity awareness; the benefits of awareness, education and training; and the importance of knowing the level of awareness of officials within the research focus area will also be discussed. Problem and thesis statements are defined together with research objectives (both secondary and primary), with delineation defining the boundaries of the research and research approach to be followed.

1.1 Workspace environment and Cybersecurity

Today organisations use the Internet as a source of information and a vehicle through which information is exchanged and transactions are concluded. According to World Internet Users and 2018 Population Stats, the number of Internet users has grown to include up to 54.4% of the world population (Internet world stats, 2017). Internet usage has grown so much that mobile devices such as cellphones, tablets, laptops, and smartphones, which are widely used by individuals for both business and personal purposes, are now connected to these interconnected networks. There is a negative aspect to these mobile devices within organisations as employees can misuse them, and security holes can be opened since IT departments have less control over the external networks; moreover, information processed on these external end-points is relatively difficult to control and manage (Silic & Back, 2013).

Cyberspace brings with it challenges in that the overall environment is controlled by no one; it has no boundaries. Cyberspace enables e-commerce. It has distinct characteristics such as anonymity, lack of security, consumer victimisation, and weak control (Oates, 2001). Anonymity allows criminal activities by faceless people, individuals and employees; lack of security allows hackers to exploit vulnerabilities and to do as they wish, while consumers are exposed to losses such as privacy, funds, and personal information falling into the hands of criminals. Given all these aspects of cyberspace, organisations need to establish some cybersecurity mechanisms for the organisation and its officials in order to survive these cyber risks. The effectiveness of these cybersecurity mechanisms depends on awareness, expectations, behaviour

towards risk taking, experience with negative outcomes, and policy compliance of senior management and officials (Higgs, Pinsker, Smith, Young, 2016).

The cyber risks lead to loss of confidentiality, loss of integrity and unavailability of information. The impact of these risks include business disruptions, loss of reputation, lawsuits, loss of revenue and potentially, business closure. The cyber risks manifest themselves in many ways. Examples include phishing: this is a type of electronic mail (email) attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering (ISACA, 2016). Phishing emails target multiple employee levels, from general employees, to middle managers, to executives, and many phishing emails involve an attempt to trigger an emotional, rather than a logical, response (Harrison, Svetieva & Vishwanath, 2016). A virus is malicious software that attaches itself to other software; ransomware is a type of malicious software designed to block access to a computer files until a sum of money is paid; denial of service is an act by a criminal, who floods the bandwidth of the victim's network and fills his email box with spam mail, depriving him of services; and hacking is an illegal intrusion into a computer system and/or network.

As a cost-effective way of combating the above-mentioned attacks, employees are required to have some level of knowledge regarding these cyber risks. A programme of cybersecurity awareness, education and training, based on the known levels of current knowledge, needs to be designed and implemented within organisations.

1.2 Cybersecurity Awareness, Education and Training

Individuals who are less aware of the general operations of cybercriminals are more likely to fall victim to cybercrimes (Harrison et al., 2016). It is imperative to put together a programme deliberately to ensure cybersecurity awareness for employees and all other cyberspace users within the organisation. Individuals respond differently to stimulations; therefore, it is important to try to understand the different ways people respond to different methods and actions used in order to increase cybersecurity awareness (Siponen, 2000). Awareness has benefits, which will enable understanding of the actual exposure, choice of appropriate and informed responses, and integrating cyber-security risk management in daily duties (Information Systems Audit and Control [ISACA] 2009). Targeted educational efforts augment the knowledge and experience of officials and individuals. In turn, knowledge and experience protect them from falling

into the trap of cyberattacks (Harrison et al., 2016). Awareness, education and training programmes need to be tailored to the specific organisation for them to be effective (Thomson & Solms, 1998). To develop a fit for purpose programme and to derive value, a level of awareness has to be measured. The success of the programme lies entirely in knowing and understanding the gaps in awareness of the officials at different levels of the organisation.

1.3 Problem Statement

The previous paragraph argued for the importance of cybersecurity awareness, education and training programmes. While the statement holds in general, this thesis will consider it from the specific vantage point of the LEDA Group. Officials in the LEDA Group perform their daily duties in cyberspace. However, the ignorance and/or lack of understanding of officials about cybersecurity risks around them might expose the LEDA Group to cyber-attacks. This led to the problem that the level of awareness of officials regarding cybersecurity was not known. Knowing and understanding this level of awareness was a prerequisite to providing intervening education and training to officials. The implication of not knowing the level of awareness was that an argument for the nature of the intervention to ensure awareness, educate and train employees regarding cybersecurity was not possible.

1.4 Thesis Statement

It is believed that measuring the level of awareness of cybersecurity would enable the researcher to develop relevant and effective intervention. Since the LEDA Group performed some of its functions in cyberspace, it is perpetually exposed to cybersecurity risks. LEDA Group employees needed a fit for purpose awareness, education and training programme. This programme needed to target executives, IT personnel and end-users specifically. For effectiveness and relevance, the programme needed to be an improvement mode, structured and directed. To direct this programme, a tailored framework for implementation was required be developed and implemented. The framework developed enabled the agility required from the LEDA Group to respond to the ever-increasing complexity of cybersecurity risks. Measuring and understanding the level of lack of awareness enabled the establishment of a tailored framework.

1.5 Research Objectives

In order address the thesis statement, it was necessary to achieve the following primary objective: to develop a framework to direct and implement cybersecurity awareness, education and training, based on the current levels of awareness, in order to mitigate the human factor of cybersecurity risk during the day to day activities of officials. To achieve the primary objective, the following secondary objectives were required to be realised: to determine the state-of-the-art regarding cybersecurity awareness, education and training; to assess the current knowledge of officials regarding cybersecurity; and to determine the gap between state-of-the-art and current knowledge. Given these objectives, it was important to consider the delineation of the research study.

1.6 Delineation

This dissertation did not try to provide a general view of awareness, education and training of cybersecurity, but was limited to the Limpopo Economic Development Agency Group (LEDA) specifically and its subsidiaries, which included: Risima, Great North Transport, Corridor Mining Resources, and Limpopo Connexion. The research focused on the human factor aspect of cybersecurity risks, and therefore excluded technical aspects of cybersecurity risks. Within these limitations, the study was designed according to a systematic research process.

1.7 Research Process / Research Design

A full explanation of the research process is contained in Chapter 4; however, at this stage it is important to note that a design science project was being undertaken; therefore, it consisted of the following phases: a literature review to establish what people should know; and a gap analysis between what the officials know and what they ought to know in order to establish the framework. The existing testing questionnaire - The Human Aspects of Information Security Questionnaire (HAIS-Q) was used to assess the level awareness and education within the LEDA Group (Parsons, Butavicius, Calic, Panttison, McCormac & Zwaans, 2017). A sample upon which the assessment was conducted, was selected. The questionnaire focused on password management, email use, Internet use, social media use, mobile devices, information handling and incident reporting; and was conducted in terms of the human aspects – knowledge, attitude and behaviour. The results of this questionnaire and gap analysis between what the officials know and what they ought to know was utilised for the establishment of the framework.

This research took place in the real-world environment and culminated in a framework. Necessary approval was obtained from the authorities of the LEDA Group to administer the questionnaire and ensure compliance with ethical requirements.

1.8 Ethical considerations

The survey was conducted with permission of the employer, and the survey was voluntary and anonymous. The data was collected for the sole purpose of the study and was treated with the confidentiality it deserves. No data was gathered from sensitive groups. The University performed due diligence and clearance regarding ethical considerations.

1.9 Layout of the study

In order to achieve the objectives of this research following a design research approach, and finally to develop a framework for the implementation of awareness, education and training, the chapters are structured in the following manner: Chapter 2 looks at cybersecurity threats and users through a literature review, and the introduction of the LEDA Group organisation while Chapter 3 looks at the aspects of the state-of-the-art cybersecurity awareness, education and training with specific focus on the seven human and computer interface areas through a literature review. The detailed research approach is described in Chapter 4, after which Chapter 5 outlines details of the research findings once the questionnaire was administered and Chapter 6 provided argumentation for the development of the framework, while Chapter 7 summarises the entire treatise.

CHAPTER 2: CYBERSECURITY THREATS, ATTACKS AND LEDA GROUP

In Chapter 1 it was indicated that in this chapter, through literature review, cybersecurity threats and users would be looked at. The need for information would be discussed; the LEDA Group as an organisation would be introduced as this is the specific focus of the research; possible cybersecurity threats facing the LEDA Group, would be analysed; and cybersecurity and risks reports released by various organisations, and the consequences of security breaches will be looked into.

2.1 Information and security needs

Organisations need information to achieve objectives. In most organisations today, revenue and profits are increasingly driven by information and technology. Information is the life force of most organisations. Decisions are based on the information available through media established by the management of these organisations. The quality and reliability of these decisions depend entirely on the integrity of this information. As organisations seek to grow, and indeed become complex, they rely heavily on technology and information. The reliance on technology, on the other hand, is accelerated by the competitive advantage that comes with that technology.

The heavy reliance and need for quality information for decision-making requires that information be confidential, have integrity and be available (CIA). In today‘s organisations, information is stored in media connected to cyberspace, such as servers, laptops, desktop, tablets, iPad, smartphones, etc. Cyberspace has distinct characteristics, anonymity, inadequate security, consumer victimisation, and weak control (Oates, 2001). The characteristics of cyberspace need to be analysed and understood as they have a potential impact on the CIA of information. Employees using information in their organisations perform their daily duties within the distinct characteristics of cyberspace. The reality of cybersecurity risks is demonstrated by annual reports commissioned by cybersecurity organisations and experts.

2.2 Analysis cybersecurity 2017 reports

These reports give an indication of current threats that the LEDA Group might be facing and understanding these threats will help the LEDA Group to better prepare awareness content required for the employees to behave in cybersecurity appropriate manner. The impact of these threats, should they become a reality, is taking away the confidentiality,

integrity and availability of information and making it difficult to achieve objectives as discussed in the paragraph above. The threats attack in various ways including media such as emails, spyware, hiding behind Internet, phishing, etc.

The Cisco report 2017 observed that business email has become a highly lucrative threat vector for attackers; spyware was preferred for stealing user and company information; the Internet of things (IoT) – there is a lack of visibility in terms of not knowing what IoT devices are connected to their network; spam emails use user interaction to infect systems; supply chain attacks come through vendors' downloaded software; there are hackers; and a poor management of privileged user accounts exists.

According to the Anti-Phishing Working Group 3rd quarter 2017 report, there was a total of 6431 detected attacks, as shown in Table 2.1. Table 2.2 depicts the number of phishing sites detected in the 3rd quarter of 2017 (Ant-phishing working Group, 2017). The LEDA Group is exposed to all of these type of attacks; therefore, awareness of users within the LEDA Group is critical.

Table 2.1: Details of the detected attacks

Type	Total for July, Aug and Sep 2017
Malware C&C	15
Malware	518
Proxy auto-configuration files	1
Paid Search Phishing	1
Pharming	30
Phishing	430
Malicious Proxy Servers	58
Redirect	511
Social Media Scams	1 909
Scam Web sites	2 562
Mobile App Scam	396
Total	**6 431**

Table 2.2: Number of phishing sites – Cisco Report 2017

Month in 2017	No of phishing sites detected
July	60 232
August	73 393
September	57 317
Total	**190 942**

The Cisco Midyear Cybersecurity Report 2017 identified eight (8) impacted industries in South Africa and globally. The South African economy is reportedly losing as much as R1 billion annually owing to online activities. These industries include space where the LEDA Group operates – finance. This shows that the LEDA Group is exposed to cybersecurity risks as much as other organisations in the country. Literature has, however, shown that users of information could be the strongest or the weakest link when coming to cybersecurity. Employees should play active role in the prevention of attacks and the maintenance of the CIA of information.

The co-ordination of activities to ensure the CIA of information is performed by employees in organisations. In a nutshell, cybersecurity incidents that may affect the LEDA Group, including compromising of employee records, theft of "soft" intellectual property (e.g. information such as processes, institutional knowledge, etc.), loss or damage of internal records, compromising of customer records, compromising of business email, etc., may be prevented through appropriate knowledge, attitude and behaviour of employees within the Group. The shape, culture and nature of the Group should support its ability to attain and maintain the appropriate cybersecurity knowledge, attitude and behaviour.

2.3 The Limpopo Economic Development Agency Group

The LEDA Group is the research focus, and therefore understanding the shape, structure, size and role of the LEDA Group provides a critical context to the study. It is within this context that this research is to develop intervention for cybersecurity awareness with the Group. The LEDA Group came into being after the amalgamation of four entities in December 2012. It is a provincial economic development agency and it

is under the Executive Authority of the Member of Executive Council (MEC) for Economic Development, Environment and Tourism.

The mission of the Group is:

To accelerate economic growth, development and job creation in the province, by:

- *Promoting industrialisation;*
- *Facilitating increased trade and investment; and*
- *Supporting the development of sustainable enterprises.*

The strategic objectives are identified as follows:

- *Accelerated industrialisation in the province through strategic economic development interventions;*
- *An increase in sustainable enterprises in targeted sectors of the economy;*
- *Centres of technical and business training excellence that develop skills for the economy;*
- *An increase in trade and investment in targeted sectors in the province;*
- *An increase in access to socio-economic development through innovative products and services offered by the Group's subsidiaries and tertiary divisions; and*
- *Sound corporate governance and high performing organisation.*

The company established several divisions: finance, properties, corporative services, enterprise development and finance (EDFD), risk management and internal audit; Information, Knowledge and Projects Management (IKPM) and subsidiaries in mining, transport, housing loans, ICT Company and a life insurance company as depicted in Figure 2.1, in order to achieve its mission. The group deployed an asset base of over R1.5 bn and a staff complement of over 600 employees, as shown in Tables 2.3 and 2.4 to implement activities towards its objectives.

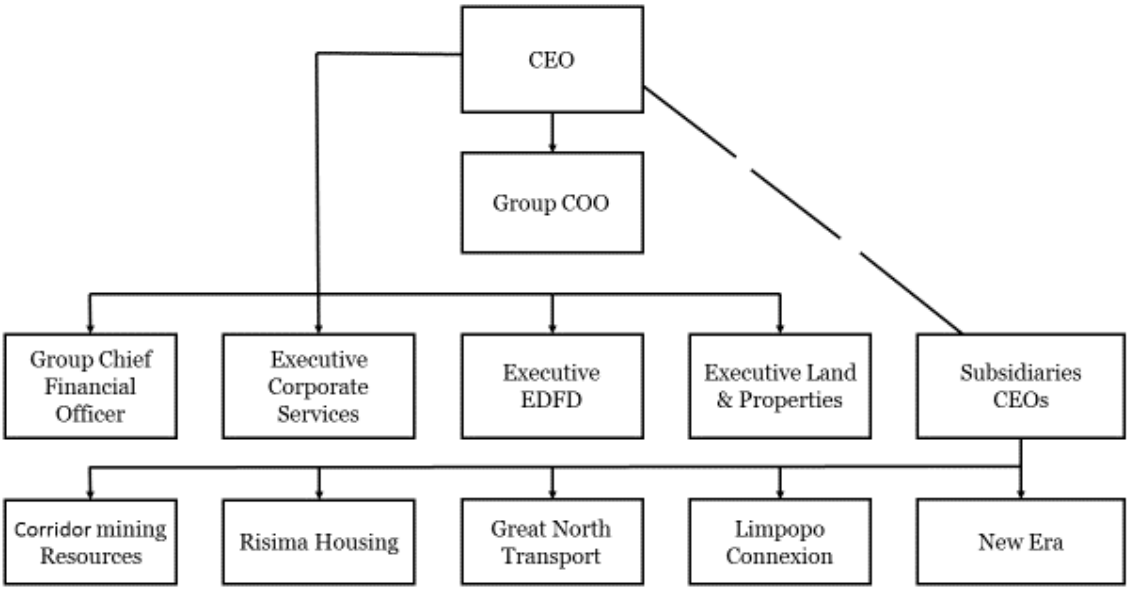

Figure 2.1: LEDA organisational structure

Table 2.3: Summary of LEDA Balance Sheet 2016/17

Details	ZAR
Biological Assets	2 117 760
Investment Property	187 624 792
Property, Plant and Equipment	405 063 936
Intangible assets	96 109 721
Investments in Associates	107 526 099
Other financial assets	532 053 063
Environmental deposits	33 734 223
Current Assets	328 039 551
Total Assets	**1 692 269 145**

The investment property consists of a factory rental portfolio where client companies rent space to carry out their businesses. This portfolio contains the personal information of tenants and their legal persons. Investment in Associates are minority investments that the LEDA Group holds in other companies. This portfolio contains information relating to other companies. Other financial assets are business loans to companies and housing finance loans to individuals. This portfolio contains the personal information of clients. A breach in security may mean that personally identifiable information could get stolen or compromised. This may lead to law suits, loss of revenue from rental clients as they leave the LEDA Group rental properties, loss of revenue from housing finance as clients switch bonds to other financial institutions, loss of reputation, and potential collapse from an inability to recover from the incident. The LEDA Group generated a total revenue of R 1.027 bn during the 2016/17 financial year. Security breaches could wipe out the revenue generated from the above assets.

Table 2.4: Group Staff Profile

Employee Level	Establishment
Top Management	12
Senior Management	45
Professionally Qualified	126
Skilled technical and academically qualified	217
Semi-skilled	188
Temporary and Interns	30
Total	**618**

Including top management, over 400 employees are using either a laptops, desktops, mobile phones, smart phones or iPads, or laptops and mobile phone/smart phone. These devices are connected to cyberspace. Most, if not all, pose risks to cybersecurity. The awareness level of employees about cybersecurity is not known.

Different systems, as shown in Table 2.5, are used in the Group to enable day-to-day operations and to enhance efficiencies. The application of these systems requires employees to use work computers or devices connected to cyberspace with exposure to potential cyber-attacks. The eventuality of the attacks largely depends on the behaviour of the users; a therefore, user awareness is key to the prevention of such possible attacks. These systems were purchased from vendors who provide operational support, which

service places the LEDA Group information in the hands of third parties, leaving LEDA with less control on such information. The third party arrangement increases the chances of attacks as threats such as viruses may be introduced into the network by employees of the third party; malware may come through connectivity to the third party network; and hackers may obtain the important information they require to hack the systems through data held by the third party.

Table 2.5: Information systems within the LEDA Group

No	User/Division	Brief description of use	Typical Information
1	Finance	Recording of financial transactions	Accounting records
2	Finance	Preparation of Financial Statements	Accounting records
3	Finance Properties Development Finance Housing Finance	Rental and properties revenue Rental administration Business Loan administration Home loan administration	Client personal details
4	Supply Chain Management	Procurement of goods/services	Service provider's details
5	Payroll	Payroll administration	Employee personal details
6	Leave	Employee Leave administration Subsistence and Travel Claims	Employee's personal details
7	Internal Audit	Audit administration	Company Information
8	Training and Skills Development	Student administration	Student's personal details

The responsibility for cybersecurity currently resides in the IT division with the structure depicted in Figure 2.2. The lack of positions such as Chief Information Officer, an Information Security Programme Manager creates a vulnerability to cybersecurity of the LEDA Group in that the responsibilities regarding the co-ordination of cybersecurity, the development of an overall strategy for the cybersecurity awareness, education and training programme, and the implementation of an awareness, education and training programme, which is normally distributed between Chief Information Officers and Information Security Programme Managers were not formally allocated to any position in the existing structure depicted in Figure 2.2.

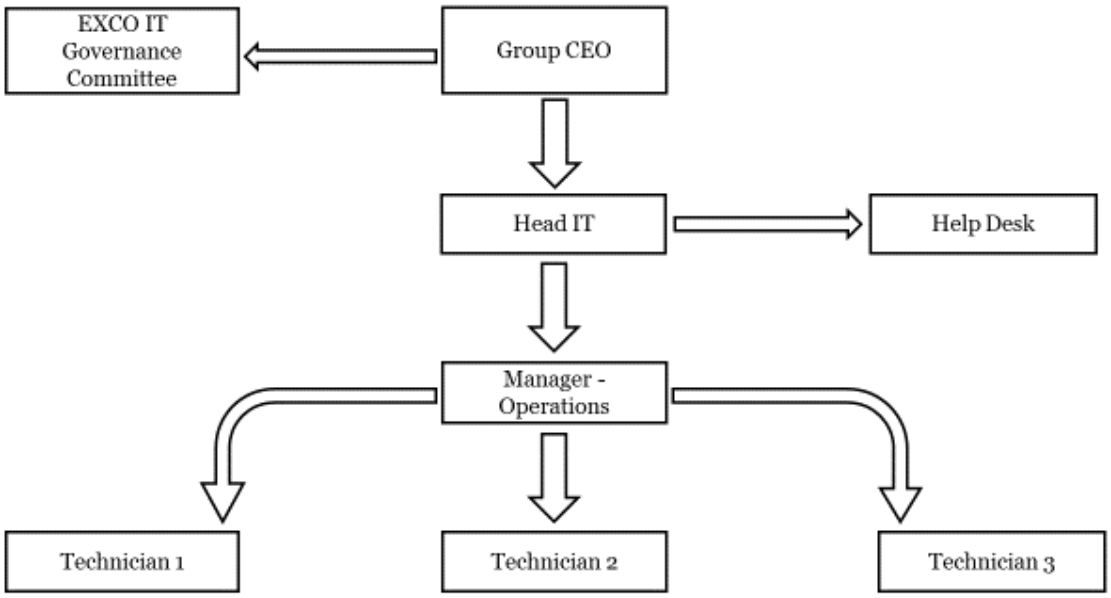

Figure 2.2: IT structure – LEDA Group

2.4 Threats to the LEDA Group vulnerabilities

The objectives of the LEDA Group, the top management structure, the IT structure, the cybersecurity reports analysed by experts, and the structural vulnerabilities of the Group to cybersecurity was noted in the above paragraphs. The Group, like all organisations in the information space, face real-world cybersecurity threats. These attacks lead to potential loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability. A vulnerability is a weakness or gap in the protection efforts. A threat is an action, a potential action, or inaction, likely to cause damage, harm or loss. Cyber-attacks are aggravated by the key characteristics of cyberspace: anonymity; weak controls, and

user awareness or knowledge; as well as attitude and behaviour. Anonymity and weak controls allow criminals to carry out criminal activities with the 'security' that they are unknown and that it would be difficult, if not impossible, to trace them. Users fall prey to criminals owing to their lack of understanding of how cyber criminals operate, as well as owing to the natural inclination of users to trust. Although the Internet supports business, cyber criminals also use the Internet to carry out their cybercrimes. Employees and business processes within the Group rely on the Internet for their daily activities; therefore, employees of the Group are equally vulnerable to the activities of criminals as mentioned above in this paragraph. According to World Internet Users and 2018 Population Stats, the number of Internet users has grown to include up to 54.4% of the world population (Internet world stats, 2017). This use of the Internet presents cybercriminals with opportunities for reaching potential targets. The employees within the Group are part of these Internet users and their natural inclination to trust exposes them to email phishers, social engineers and hackers. Internet use brings with it viruses, ransomware, etc.

2.4.1 Phishing and Social engineering

In the LEDA Group, more than 400 employees interface with computers in performing their duties on a daily basis. They receive emails on these computers and, in some cases, they also receive emails on laptops, cellphones and iPads. Some cybercriminals use emails as a medium of attack, which is called phishing, and other means of social engineering. Phishing is an attempt to obtain access to sensitive information by disguising it as a trustworthy entity in an electronic communication (Heartfield & Loukas, 2018). Many phishing emails involve an attempt to trigger an emotional, rather than a logical, response (Harrison et al., 2016). Phishing thrives on the basic belief that the weakest link in cybersecurity is the human user (Safa & Solms, 2016). It attempts to exploit the user-computer interface as, through this, even the strongest technical protection systems can be bypassed by manipulating the user into divulging a password, opening a malicious email attachment, or visiting a compromised website (Heartfield & Loukas, 2018). The knowledge, attitude and behaviour of the user is key to this risk. Information processing style, email knowledge and experience supports susceptibility to phishing (Harrison et al., 2016). While both phishing and social engineering exploit human psychology and behaviour patterns, social engineering is more focused, and specifically targeted. Perpetrators invest time, energy and resources in gathering

intelligence on their intended victims through, among others, company profiles, employment lists, social media, etc. before launching an attack. Phishers and social engineers are looking for personally identifiable information (PII), as this is the key to information systems and networks. The LEDA Group utilises systems, as outlined in the paragraphs above, and these systems contain information including personal information for which processing is required to comply with the Protection of Personal Information Act (POPIA), and the right to privacy as required by Section 14 of the South African Constitution. To prevent a breach of cybersecurity from these threats requires that the LEDA Group employees are able to recognise phishing and social engineering emails. Inability to recognise such emails will lead to employees opening them and falling prey to criminals; and therefore, compromising security. The impact of the data breach may lead to loss of clients; meaning loss of revenue from rental of properties, housing loans, business loans and other services; laws suits by clients resulting in loss of reputation; and therefore, loss of market share.

2.4.2 Hacking

Hacking means an illegal intrusion into a computer system and/or network. Hackers use psychological manipulation to lead and influence the other person into giving up the required information such as personal information and credentials. According to Gold (2011), hackers use the science of neuro-linguistic programming (NLP) where *neuro* refers to conscious and unconscious thought processes; *linguistic* refers to the way in which people use language to make sense of their experiences; and *programming* refers to the way to achieve the results you want and the impact you have on yourself and on others. To counter the threat of being hacked, organisations need to apply the science of NLP as well, to psyche the employees in addition to the technical tools they provide. Organisations need to create knowledge that will turn into common sense, which will prevent the exploitation of hackers targeting computer systems and network users.

2.4.3 Viruses

It has been seen in the above paragraphs that the LEDA Group is dependent on information to carry out its business. Integrity and the availability of information is key in order for activities to be carried out and for decisions to be made. Viruses are a threat to the integrity and availability of information, also for the LEDA Group. A computer virus is a malicious computer program that can copy itself and infect other computers

(Zhu, Yang, & Ren, 2012)). USB drives, external hard drives, mobile phones, networks, etc. have become the main means of infection transmission. Users are the bridge between the computer and these devices; therefore user knowledge, attitude and behaviour become critical in the spread of virus in the organisation. Once a virus is in the network, it spreads. Some viruses, such as Trojan horses camouflage themselves, thus inducing the users to download those (Han & Tan, 2010). Han & Tan (2010) show that in 2003, the virus called King attacked the global world so that Internet users could not send or receive emails, book aeroplane tickets, or use credit cards to pay for anything. The consequences of a virus attack may be devastating to the LEDA Group because when the information is not available owing to a virus attack, business activity stops, revenue generation activities stop. The information processed in systems outlined in Table 2.5 will lose integrity once attacked by viruses, and decisions based on such information will lose authority. The LEDA Group employees are required to recognise when their computers and communication devices are under attack, as this may help the prevention of large-scale attack and subsequent total shut-down.

2.4.4 Ransomware

It was noted in the preceding paragraphs that the LEDA Group is dependent on information to carry out most of its activities. It also stores and processes personal information which is sought after by hackers. It is therefore common knowledge that the LEDA Group cannot afford to lose or not have access to its information asset. Ransomware is a type of malicious software designed to block access to computer files until a sum of money is paid. Hampton, Baig, and Zeadally, (2018) noted that ransomware infections have grown exponentially during the recent past to cause major disruptions in operations across a range of industries including governments. Ransomware is driven by its ability to conceal the perpetrator, ensuring anonymity, anonymous payment capability through Bitcoin, and strong encryption (Hampton et al., 2018). The ransomware software infects a victim's machine when the naïve victim opens an attachment that accompanies a spam message or when the victim accesses a compromised website (Fimin, 2017). Employees require some level of common knowledge of the organisation to mitigate a ransomware attack within a short time period of the attack in order to isolate the affected machine from the network before ransomware spreads.

2.4.5 Use of the Internet and cybersecurity

More than 400 employees in the LEDA Group are connected to the Internet. The Internet provides the employees with much information to supplement and support their efforts to achieve their allocated responsibilities. Although the Internet is the greatest invention, it provides a vehicle for cybercrimes. The 54% (over 4 billion people) of Internet users do not know each other; they are dispersed all over the world; boundaries are irrelevant to them; and they are regulated through different laws; users are anonymous. The anonymity provides an opportunity for cybercriminals to carry out cybercrimes, such as the unlawful securing of access to data, computer programs, computer data storage media or computer systems; the unlawful acquiring of data; unlawful acts in respect of software or hardware tools; the unlawful interference with data or computer programs; the unlawful interference with computer data storage media or computer systems; and the unlawful acquisition, possession, provision, receipt or use of passwords, access codes or similar data or devices (Department of Justice, 2017), with a lesser threat of being caught. From the user angle, the Group is susceptible to these crimes manifesting themselves in many forms including phishing, hacking, viruses and ransomware, as discussed in the previous paragraph. Lack of awareness or understanding of these manifestations by employees becomes the real source of cybersecurity risks. The cybersecurity control of organisations is limited to the network of such organisations. The interconnectedness of networks complicates and weakens the ability of organisations to exercise adequate control over what and who knocks on the door of the network of said organisations. Thomson and Solms (1998) concluded that, given this complexity, it is no longer possible to maintain effective cybersecurity with physical and technical controls alone.

2.5 Potential impact of cybersecurity breaches to the LEDA Group

There are negative consequences of security breaches. They include reputational damage, loss of revenue, law suits, etc. In the case of the LEDA Group, client and employee information is stored in the systems and this information is therefore exposed to theft if appropriate security measures are not taken. The rental, business loan and home loan systems' stored process information is protected by POPIA (Department of Justice, 2013) and the Constitution, as discussed in the preceding paragraphs. If the LEDA Group loses this information to cybercriminals, its revenue and market share are likely to shrink. Law suits may reduce the Group's financial assets. The client information is protected by the

South African Constitution under the Bill of Rights and the Protection of Processing of Personal Information Act. The reputation of the Group will suffer immensely if services provided by the Group cannot be accessed owing to issues such as the denial of service, as a result of hackers demanding ransomware, or a virus attack. All activities outlined in Table 2.3 can be shut down resulting in loss of productivity, since employees will be idle during this time.

2.6 Role of employees in cybersecurity

Employees are key in any information systems as they interface with the machines and make the systems works. However, from the literature review, it is clear that these employees may become liabilities in cybersecurity through errors, ignorance, by intention or by mistake. In this context, the LEDA Group employees have a critical role in cybersecurity within the Group. It is therefore important that the LEDA Group should implement a programme which would influence the attitude and behaviour of its employees. This programme should impart specific and tailored knowledge relating to areas exploitable by malicious attacks or to opportunities for errors during the interfacing of employees and machines. Such focus areas should include password management, email use, Internet use, social media use, mobile devices, information handling, and incident reporting. According to the Conscious Competence Learning Model, there are four levels of awareness through which employees should go in order to achieve appropriate cybersecurity knowledge, attitude and behaviour (Broadwell, 1969). The levels are: unconscious incompetence – the employee does not realize that he/she does not know how to do certain things; conscious incompetence – the employee is aware that he/she is incompetent to do his/her job securely; conscious competence – the employee knows what to do and how to do it to ensure that his/her job is done in a secure manner, but the employee stays conscious of it and still needs to concentrate in order to perform the necessary procedures correctly; and unconscious competence - the employee will not think about doing his/her job securely, but it will be part of his/her natural behaviour. Table 2.6 depicts examples of good and bad cybersecurity behaviour per focus area (Parsons et al., 2014). The LEDA Group cybersecurity awareness, education and training programme should move employees from their current level to the unconscious competence level.

Table 2.6: Good and bad cybersecurity behaviour

No	Area	Good behaviour	Bad behaviour
1	Password management	Passwords are composed to make it difficult to guess them Passwords are created and managed in a manner that the confidentiality of information cannot be compromised Passwords are changed regularly Passwords are kept secret	Use of names, birthdays as passwords Sharing passwords Using one password for different accounts
2	E-mail use	Resisting email attachments from unknown sources	Opening email attachments from unknown and suspicious senders
3	Internet use	Using only authorised software Not downloading audio and video files for personal use Cookies which share information with other websites should be deactivated Compliance with Copyright Act	Downloading video content to a work computer via peer-to-peer file sharing Visiting unauthorised websites Downloading unauthorised softwares Non-compliance with Copyright Act
4	Social media use	Not accessing social networking websites during work time Use of different passwords for work and social media accounts Privacy settings for social media accounts	Posting sensitive information about the workplace on social networking sites Use of employer resources for private social media activities
5	Mobile devices	Sending work emails using only secure networks Securing mobile devices when not attended	Configuring a wireless gateway that gives unauthorised access to the company's network Sending employer information using public Wi-Fi VPN usage when using unknown networks
6	Information handling	Following rules in saving data regularly, not leaving sensitive information on your screen, removing of corporate data, rules for storing information on diskettes, USB, hard drives, encryption, decryption, data back-up guidelines, and the disposal of information.	Disregard of established protocols regarding information handling
7	Incident reporting	Following procedures regarding incident reporting Reporting incidents	Non-compliance to incident reporting policy and procedures

2.7 Conclusion

In this chapter it has been seen that the business activities of the LEDA Group depend on information technology to a great extent. Key business activities, such as rentals, business loans, house loans, finance, payroll, supply chain management, and internal audit are driven through information technology. The Group has more than 400 employees working in the cyberspace on a daily basis. The cybersecurity and risk reports developed by industry experts have been analysed and these reports yielded insight as far as the real threats faced by the LEDA Group as far as cybersecurity is concerned. These threats were further analysed for their nature, impact and human interface vulnerabilities. It became clearer from the analysis of these threats, and the interface of the employees and computer, that employees are key in cybersecurity. Therefore, employees are required to possess some level of awareness in terms of the seven identified focus areas. To this end it is imperative to determine a benchmark for the level of awareness, education and training required for employees to play their rightful role in the security of information. In Chapter 3 the state-of-the art cybersecurity awareness, education and training will be looked at through a literature review.

CHAPTER 3: CYBERSECURITY AWARENESS - A BENCHMARK FOR LEDA GROUP

As noted in Chapter 2, employees are key to cybersecurity within the LEDA Group. Employees must have an adequate and appropriate level of cybersecurity awareness. Cybersecurity should be integral part of the responsibilities of employees working with computers and other devices connected to the network. It is through a dynamic cybersecurity awareness, education and training programme that such cybersecurity responsibility could be economically, efficiently and effectively achieved.

In this chapter, the best cybersecurity awareness, education and training programme building blocks will be discussed through literature review. The discussion includes the manner in which the programme should be packaged so that the content is targeted to employees in the context of their responsibilities, and aims at changing the attitude and behaviour of the employees (Siponen, 2000). This chapter also discusses how the LEDA Group could ensure that employees using, managing and directing technology and information understand their role and responsibilities relating to the LEDA Group's information asset security.

The discussions revolve around the seven focus area identified in Chapter 2, namely, password management, email use, Internet use, social media, mobile devices, information handling and incident reporting.

3.1 Role of governance in the cybersecurity awareness, education and training (CSAET) programme

Success of the CSAET programme depends on key positions within the organisation (Eberhagen, Giannakopoulos, Marinagi, Metalidou, Skourlas, & Trivellas, 2014 and the same is true for the LEDA Group. If the LEDA Group needs success in the implementation of the CSAET programme, the Chief Executive Officer (CEO) must ensure that adequate resources are prioritised for CSAET. Resourcing should cover the implementation of an appropriate cybersecurity programme with a strong awareness, education and training component.

In order to achieve the goals of CSAET, the CEO should appoint the Chief Information Officer (CIO) or equivalent, assign responsibility for cybersecurity, monitor that the LEDA Group-wide cybersecurity programme is implemented, is well-supported by

resources and budget, and is effective. The CIO should be tasked to administer training; to oversee personnel with significant responsibilities for cybersecurity; and to work with the Group‘s Information Security Programme Manager to establish an overall strategy for the cybersecurity awareness, education and training programme (Da Veiga & Martins, 2017). The CIO should ensure that the CEO, senior managers, system and data owners, and others understand the concepts and strategy of the cybersecurity awareness, education and training programme, and are informed of the progress of the programme’s implementation; should ensure that the organisation’s CSAET programme is funded; should ensure the training of the organisation ‘s employees with significant security responsibilities; should ensure that all employees are sufficiently trained in their cybersecurity responsibilities; and should ensure that effective tracking and reporting mechanisms are in place.

The Information Security Programme Manager has tactical-level responsibility for the CSAET programme and should ensure that CSAET material developed is appropriate and timely for the intended audiences (Yoo, Sanders, & Cerveny, 2018). In addition, the Information Security Programme Manager should ensure that CSAET material is effectively deployed to reach the intended audience; should ensure that employees and managers have an effective way to provide feedback on the awareness, education and training material and its presentation; should ensure that CSAET material is reviewed periodically and updated when necessary; and should assist in establishing a tracking and reporting strategy.

For the CSAET programme to realise its objectives, other managers within the Group have responsibility for complying with CSAET requirements established for employees under their supervision (Barton, Lane, Tejay, & Terrell, 2016). Managers should work with the CIO and Information Security Programme Manager to meet shared responsibilities; serve in the role of system owner and/or data owner, where applicable; consider developing individual development plans (IDPs) for users in roles with significant cybersecurity threats responsibilities, promote the professional development and certification of the information security programme staff, security officers, and others with significant security responsibilities; ensure that all users (including contractors) of their systems are appropriately trained in how to fulfil their security responsibilities before allowing them access; ensure that users (including contractors)

understand specific rules of each system and application they use; and work to reduce errors and omissions by users owing to a lack of awareness, education and/or training.

Users are the largest audience in the Group and are the single most important group of people who can help to reduce unintentional errors and cybersecurity vulnerabilities (Eberhagen et al., 2014). Users may include employees, contractors, others requiring access. Users must understand and comply with the Group's cybersecurity policies and procedures; be appropriately trained in the rules of behaviour for the systems and applications to which they have access; work with management to meet training needs; keep software/ applications updated with security patches; and be aware of actions they can take to better protect the Group's information asset. These actions include, but are not limited to, password management, email use, Internet use, social media use, mobile devices, information handling, data backup, proper antivirus protection, reporting any suspected incidents or violations of cybersecurity policy, and following rules established to avoid social engineering attacks as well as rules to deter the spread of spam or viruses and worms (National Institute of Standards and Technology, 2003). All these responsibilities must be directed by the Cybersecurity Policy of the Group (Barton et al., 2016). CSAET content should aim at changing the attitude and behaviour of the entire user population. In order to change the attitude and behaviour, the current attitude and behaviour should be assessed.

3.2 State of cybersecurity awareness assessment

The first step in cybersecurity awareness, education and training of employees is the assessment of the current state within the Group (Parsons et al., 2017), what risks need to be addressed; what challenges a new or improved CSAET programme could face, and what Group-specific factors need to be included as part of the training. A tested questionnaire based on research could be used to assess the state of awareness regarding cybersecurity (Parsons et al., 2013, 2014, 2017). This assessment is a continuous activity which happens throughout the programme. The imperative of continuous assessment exists to offer the programme the ability to address the emerging threats, new regulations, and shifting employee knowledge quickly. The results of the assessment inform the content of cybersecurity awareness, education and training programme. The programme content should be differentiated in response to the findings and analysis of the assessment.

3.3 Cybersecurity awareness, education and training material development

The content of the programme should be weighted to fit the pre-knowledge of the employees within the Group. The developers and facilitators of the programme should aim at winning buy-in from employees (trainees). This will go a long way in enhancing the acceptance and ownership of the programme by employees (Yoo et al., 2018). The programme must be effective in changing the attitude and behaviour of the users. The pedagogy should build in soft-skills to gain and retain the attention of trainees during programme implementation. The benefit of having an employee who is cybersecurity aware, educated and trained is successfully ensuring confidentiality, integrity and the availability of information during the performance of his/her duties (Eberhagen et al., 2014). Chapter 2 identified seven areas which, in combination, represented the minefield of cybersecurity threats and vulnerabilities including: password management, email use, Internet use, social media use, mobile devices, information handling and incident reporting. The content of CSAET should enable users to carry out their daily activities effectively in a cyber-secure way within these minefield.

3.3.1 Password management

A password is a key to an information kingdom. A password is like a signature or a fingerprint; it ensures the authenticity of the user in order to ensure that unauthorised users do not gain access to the computer, device or network (Gafni, Pavel, Margolin, & Weiss, 2017). Cybercriminals need the password in order to commit cybercrime without being noticed. Passwords should be composed to make it difficult to guess them (Shay, Komanduri, Durity, Huh, Mazurek, Segreti, Ur, Bauer, Christin, & Cranor, 2016). Given the importance of information assets, it is key that passwords should be created and managed in a manner that the confidentiality of information cannot be compromised. According to Shen et al. (2016), it remains a fact that users need to get guidance from somewhere, and ideally be supported in handling the burden of password management.

CSAET is a way of providing that user guidance and support for password management. CSAET should provide guidance about how a good password is chosen and what should not be chosen as a password. It should provide examples to demonstrate the composition of good passwords. Examples of how to choose good passwords include using non-personal information. Group employees should be aware that passwords

should not use meaningful personal information such as the user's name, surname, nickname, date of birth, ID number, telephone number or any other aspect that may be associated with the user. Use uncommon information: passwords should not use words that can be found in dictionaries, acronyms or common permutations. Use a combination of characters. Use a combination of uppercase and lowercase letters as well as numbers when creating passwords; ensuring sufficient length. Passwords should be at least eight characters long, ensuring uniqueness. Use unique passwords that are not used for other purposes and correlate complexity with risk. Vary the complexity of the password to match the risk associated with its use (Shen, Yu, Xu, Yang, & Guan, 2016; Bryant & Campbell, 2006; Butler & Butler, 2015). Once a good password is chosen, password management rules must be followed, and these rules include single ownership. Group employees should be aware that passwords should be kept secret and not be disclosed to or shared with other persons, and they must be regularly changed. The shorter the lifetime of a password, the better; and it must be kept safe. Group employees should ensure that passwords are not written down or stored in places where they could easily be discovered; and should be used only once Group employees should understand that their password is a treasure to individuals who need to compromise the information of their organisation.

There are many different methods used to compromise password security, some of which are unsophisticated requiring little or no technical knowledge, while others require a high level of technical expertise. Unsophisticated techniques include guessing, observing, viewing written records, being told, tricks and artifice and even sifting through rubbish bins (Bryant & Campbell, 2006). It is therefore their responsibility to protect the information by protecting their passwords.

3.3.2 Email use

In order for employees to protect Group information asset from threats such as phishing and social engineering, as discussed in Chapter 2, employees must be aware of cybersecurity issues brought about by email use. Email communication is growing as the main method of communication for individuals and organisations (Kruger, Drevin, & Steyn, 2007). On the other hand, it is also growing as means of conducting cybercrimes e.g. data theft, identity theft, virus, malware, and ransomware attacks, etc. Cybercriminals use the email to prey on access to networks from vulnerable users by

sending phishing and social engineering emails. Phishers and social engineers apply their tactics in order to be given the information they are after, by the user (Harrison et al., 2016). The email sent to the user is either enticing the user by offering a reward at the other side of the action by the user; which action will provide the information required by the phisher; or the email threatens the user by showing the adverse impact to the user if the action required by the phisher is not taken immediately. The aim is obtain personally identifiable information (PII) (Arachchilage & Love, 2014). The keepers of this personally identifiable data are the targets of the phishers; they need access to this data.

Cybercriminals know that almost any employee can give them access to the organisation's network (Futcher, Safa & Solms, 2016). HR managers are vulnerably positioned for phishing criminals as they are the custodians of PII. Executives are targets for which cybercriminals tailor emails. This is because of the privileged nature of their responsibilities in organisations. The targeted categories are not limited to the three mentioned above and this is confirmed in the Email Security Social Engineering Report, 2016, in which, according to the FBI, between October 2013 and May 2016, law enforcement globally received 22 143 reports of business email compromise, resulting in $3.1 billion in fraud losses. Since January 2015, the FBI has seen a 1300 per cent increase in victims and losses. CSAET on this focus area should factor this reality in when developing material for the email focus area.

In developing CSAET material, the developers should identify and differentiate between the vulnerable groups. The development of the material should address differentially identified categories. Examples of phishing emails should be unpacked in the CSAET material. This should give practical illustration of what the user should be aware of, and should know when receiving emails, and how to spot a phishing email (Harrison et al, 2016). To protect Group information assets from phishers and social engineers, users should be able to spot a phishy email; should own the responsibility to prevent phishers and social engineers from gaining access to information asset (Yoo et al., 2018); and must understand the impact of cybersecurity breaches to themselves and to the LEDA Group they are serving. To be effective, CSAET material should be based on an analysis of the pre-knowledge of the differentiated users within the Group.

3.3.3 Internet use

As discussed in Chapter 2, Internet use is pervasive and its use is growing incredibly fast. CSAET should educate the Group employees about appropriate use of the Internet. Group employees should be made aware of such appropriate and inappropriate use or behaviour. Group employees should be aware that using the Group's resources to download audio and video files for personal use is inappropriate and may lead to disciplinary proceedings; cookies which capture information from your computer and share it with websites should be kept deactivated unless needed; employees should know not to reveal their entire name, full date of birth, contact details, or any other personal information to anyone; users should only conclude financial transactions from reputable websites; copyright is a legal matter, in South Africa it is enacted through the Copyright Act and users should understand that some material on the Internet is copyrighted and that downloading or copying may have legal implications for the organisation; unauthorised copying of software is called piracy - it is a form of theft and it is illegal.

Group employees should know that they should never download software and should only use software authorised by the Group. Group employees should use Hyper Text Transfer Protocol Secure (Https), as data is encrypted before being transmitted and therefore would not be readable when intercepted by others. Hyper Text Transfer Protocol (Http) should not be used, as data is transmitted without being encrypted and is therefore exposed to being intercepted and used by others. Group employees should be aware that software downloads from the Internet may bring viruses into the network. Once a virus is introduced into the network, it can infect USB drives, external hard drives, mobile phones, etc. (Zhu et al., 2012). Many viruses are able to email themselves to every contact in the address book of an infected computer. Group employees should be aware of types of viruses; how to realise that your computer may be infected; what to do when you suspect that your computer may be infected; and the potential impact of virus infection.

3.3.4 Social media

It is critical that Group employees use social media responsibly. Organisations, including the LEDA Group, are turning to social media as a result of its advantages in terms of audience coverage. It opens up the possibility of less expensive and more

effective online marketing and also offers new approaches to direct contact with potential customers, inspires developing business and communication strategy (Drahošová & Balco, 2017). According to Khan, Swar, & Lee. (2014), social media brings with it risks, including privacy: the potential loss of control over information associated with identity fraud, and the disclosure of organisation-kept data to third parties; social: what may be perceived as distasteful posts by employees, may impact negatively on the reputation of the Group: and time risks: social media possesses a wide variety of addictive activities. Once addicted, users tend to spend more time browsing and socializing on social network sites, and thus productivity suffers. CSAET should influence the Group employees to ensure that they use social media in a responsible manner and in compliance with social media policy. Group employees should know, understand and accept the responsibility and consequences of their actions on social media (Parsons et al., 2017). Group employees should further be made aware that their personal data available on social networks, and the personal details embedded into passwords, could facilitate password cracking, which in turn is used to log into the employees' accounts and enable unauthorised access to information (Gafni et al., 2017).

3.3.5 Mobile devices

More than 400 employees within the Group use mobile devices such as laptops, tablets and mobile phones. The multiple use of these devices is increasing within the Group (Kleiner & Disterer, 2015). These devices store sensitive information and also utilise Virtual Private Networks (VPN) connections back to the main server in the office. Each mobile device represents a potential point of compromise; therefore, it is imperative to take steps to protect these devices (Mylonas, Kastania, & Gritzalis, 2013).

Group employees need to be trained and educated regarding mobile application security, the use of public Wi-Fi hotspots, the importance of VPN usage when using new or unknown networks, PIN and passcode security, detection and avoidance of SMS style phishing attacks (smishing), and the importance of encrypting the data on their devices.

3.3.6 Information handling

Group employees should be trained and educated about the handling of information in order to achieve security of information. CSAET on this area should include data storage processes, which should cover saving data regularly, not leaving sensitive information

on your screen, removing of corporate data, rules for storing information on diskettes, USB, hard drives, encryption, decryption, data back-up guidelines, and the disposal of information.

CSAET should entrench the key behaviour of ensuring that important files and folders are backed-up, that confidential information is encrypted, understanding that it is good practice to back-up all locally stored folders and directories onto a central server on a regular basis, and that one is responsible for ensuring that all important data files can be successfully restored following any incident.

3.3.7. Incident reporting

Incident treatment procedures should be developed and Group employees should be aware of their responsibility towards incident reporting. In this focus area, Group employees should be trained regarding how to recognise an incident, the importance of reporting incidents, and the possible consequences of not reporting incidents, as well as non-compliance with the incident reporting policy.

3.4 Cybersecurity awareness, education and training programme

It is clear from the above paragraphs that the LEDA Group should put in place a CSAET programme. CSAET should be presented to the employees based on the assessment of their pre-knowledge. The contents of the programme should be targeted at the employees in terms of their role in the organisation.

Employees should be taken through the programme using differentiated methods, such as gamified training content. Employees should be continuously motivated to believe in themselves that they are equal to the task of ensuring cybersecurity, and this should be built into the pedagogy of CSAET (Aurigemma & Mattson, 2017). The presentation, regardless of the medium, should include relevant training examples and language to motivate employees. Employees should be addressed directly to gain their attention and keep it. The presentation should provide multiple practice points throughout the stages of training to keep users engaged. To achieve effectiveness in changing the attitude and behaviour of the employees, the pedagogy should apply psychological elements such as challenge, feedback, autonomy, immersion, and social interaction (Yoo et al., 2018).

The outcome of the cybersecurity awareness, education and training is cybersecurity culture ensuring confidentiality, integrity and availability of the information asset. The CSAET must change the risky culture and entrench a positive culture (Da Veiga & Martins, 2017). According to Kearney and Kruger, (2016) CSAET should manage various human aspects such as knowledge, attitude and behaviour in cybersecurity. To manage and change the attitude, behaviour and culture, the knowledge imparted by CSAET should live in the memory of employees and this could be achieved through consistent learning and re-learning (Pashler, Rohrer, Cepeda, & Carpenter, 2007). To emphasis the point of continuous CSAET, the following example may be looked at: employees work all year, facing the reality of cybersecurity risks every day; but they undergo CSAET only once or twice per year. In practical terms, they're asked to tap their knowledge of cybersecurity practices nearly on a daily basis, based on training they received months and months ago. The CSAET has its core knowledge identified in Chapter 2. The proposed framework for the implementation of CSAET programme, as shown in Figure 3.1, starts with step 1, Assess, where the cybersecurity culture, cybersecurity risks and employee knowledge are assessed. The importance of this assessment is to ensure that the CSAET programme addresses the real need of the employees. Step 2 is the Plan phase on which strategy to implement the programme that meets the gaps identified during step 1 is developed. Step 2 involves development of awareness and training material and determination of medium of delivery. Step 3 is the implementation phase where the actual education and training is delivered to employees and the final step is reinforcement. Reinforcement ensures that learning is continuous throughout the year and ultimately the desired cybersecurity attitude and behaviour are achieved.

Humans are forgetful creatures; therefore, without immediate and continual reinforcement, a high percentage of the knowledge gained in the training phase will tend to evaporate quickly (Wozniak, Gorzelanczyk & Murakowski, 1995) .A variety of means should be employed to keep training in the on-mode, such as animations, videos, games, posters, articles, etc. Year-round training and reinforcement strategies should be developed based on thorough assessment of the LEDA Group cybersecurity culture (Li, Liu, Wang, Yasin, & Zowghi, 2018).

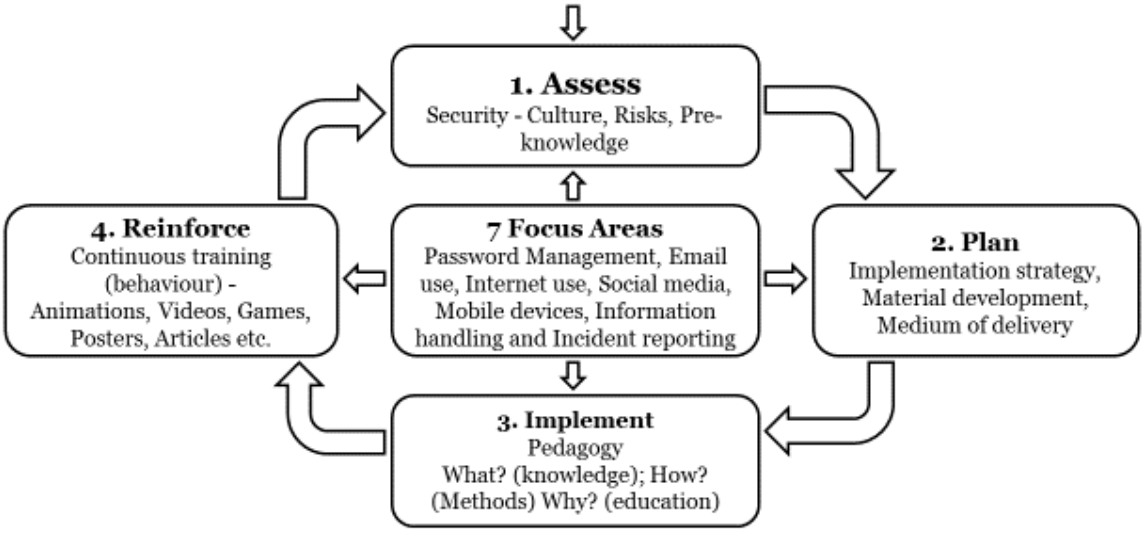

Figure 3.1: Theoretical CSAET Framework

3.5 Conclusion

In this chapter, the ideal cybersecurity awareness, education and training were discussed. This is the benchmark against which the current level of cybersecurity awareness of the LEDA Group employees would be evaluated. The mechanics of cybersecurity awareness, education and training including governance, awareness assessment and training material were analysed and synthesised. The contents of CSAET was discussed in terms of the seven focus areas of password management, email use, Internet use, social media, mobile devices, information handling and incident reporting. What is required to be known per focus area was discussed clearly in order to make it possible to test the current level of knowledge with specific standards. The pedagogical elements aiming at ensuring employees learning for retention of knowledge were also demonstrated in this chapter. The chapter concluded with Figure 3.1 which depicts state-of-the-art CSAET framework, based on a literature review. In the next chapter, research methodology and data collection methods are discussed. The methodology and research methods are required to achieve the objectives determined in Chapter 1.

CHAPTER 4: RESEARCH METHODOLOGY

As noted in Chapters 2 and 3, LEDA Group is exposed to cybersecurity attacks. The role of employees was identified and analysed with the insight of literature review. The benchmark theoretical framework for implementation of cybersecurity awareness, education and training, based on literature review was discussed in Chapter 3. The theoretical framework will be refined in the next Chapters taking the results of the research into account.

As the current level of cybersecurity awareness by employees of LEDA Group was not known, this Chapter will focus on methodology to research and assess this unknown level of cybersecurity awareness. In this chapter, the research methodology to determine the level of awareness by LEDA Group employees is outlined.

To establish and analyse the above-mentioned unknown level, Nelson Mandela University-Design Science Framework Methodology (NMU-DSFM) will be followed. The logical phases of this research methodology namely, analysis; design; evaluate, and diffuse will be discussed in the next sections.

4.1 Research Paradigm

LEDA depends on the information asset stored in electronic mediums and transmitted electronically. The devices utilised to store and transmit these information are connected to cyberspace. LEDA Group is therefore exposed to cybersecurity attacks such as phishing, viruses, hackers etc. To effectively counter these attacks, employees need to have a certain level of cybersecurity awareness and knowledge regarding these threats and mitigation. A research of level of cybersecurity awareness level must be conducted to determine the current knowledge. A gap between what is known and what ought to be known by LEDA Group employees must be analysed.

NMU-DSFM, a combination of Design-Oriented and Design-Based approaches would be followed. Design-Oriented approach aims to develop and provide instructions for actions that are practical and actions are in the form of artefact (Osterle, Becker, Frank, Hess, Karagiannis, Krcmar, Loos, Mertens, Oberweis, & Sinz, 2010). The design-oriented approach follows the principles of Abstraction which means artefact must be applicable to a class of problems in order to ensure real contribution by the research,

Originality meaning artefact must substantially contribute to the advancement of the body of knowledge, Justification which means artefact must be justified in a comprehensible manner and must allow for its validation and Benefit which means artefact must yield benefit – either immediately or in the future – for the respective stakeholder groups.

On the other hand design-based approach is a series of approaches, with intent of producing new theories, artefacts, practices that account for and potentially impact learning and teaching in naturalistic settings (Herrington, McKenney, Reeves, & Oliver, 2007). The design-based approach follows the principles of Addressing a practical/real world problem, Working within natural setting context in order to address the problem, Participation by practitioners from the natural setting, Results may be in the form of a theory, artefact or practice and Results must make contribution to both theory and practice.

The framework that will be designed for LEDA will comply with the above combination of principles and therefore will contribute in resolving the real cybersecurity awareness, education and training challenge as stated in the problem statement.

4.2 Research Methodology

As indicated in paragraph 4.1, NMU-DSFM is a combination of design-oriented and design-based approaches. Design-oriented approach has four phases as depicted in Figure 4.1. These four phases provide iterative steps to follow with a goal of developing an artefact.

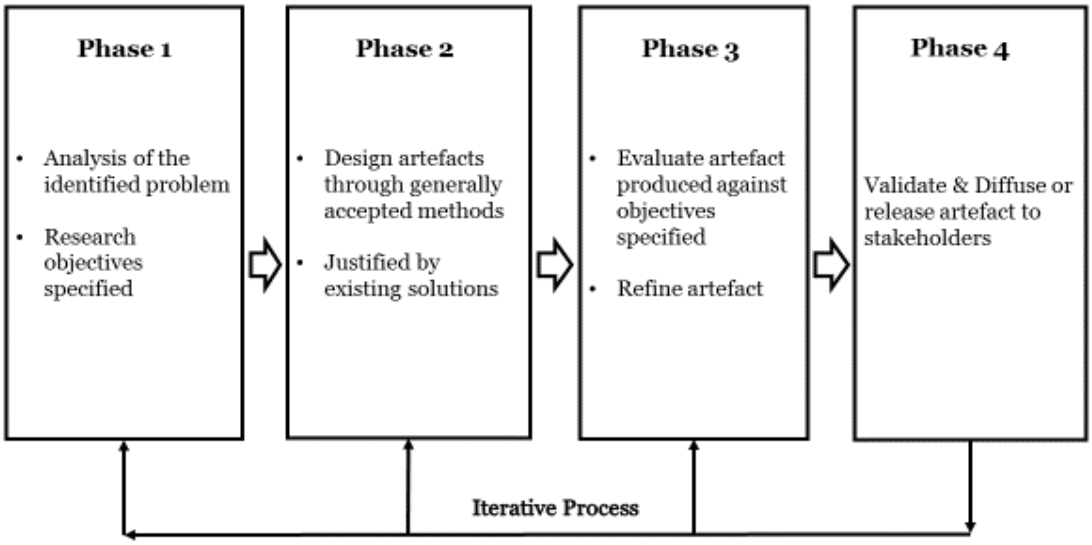

Figure 4.1: Design-oriented Information Systems Research (Osterle et al., 2010)

The design-oriented approach does not prescribe, dictate or propose comprehensive guidance to be followed, it provides academic freedom. The key for this approach is compliance with four principles mentioned above. The researcher thus has the freedom to choose the methods befitting the situation at hand.

The design-based approach also has four phases as depicted in Figure 4.2. These four phases provide steps for refinement of problems, solutions, methods and core aspects on which artefact is based. This approach will mainly be consulted to augment the design-oriented as the main approach to be applied in this research. The design-based approach provides detail on guidance to be followed. The steps depicted in Table 4.1 are consulted to supplement the design-oriented approach. The combination of the two approaches is shown in Figure 4.3.

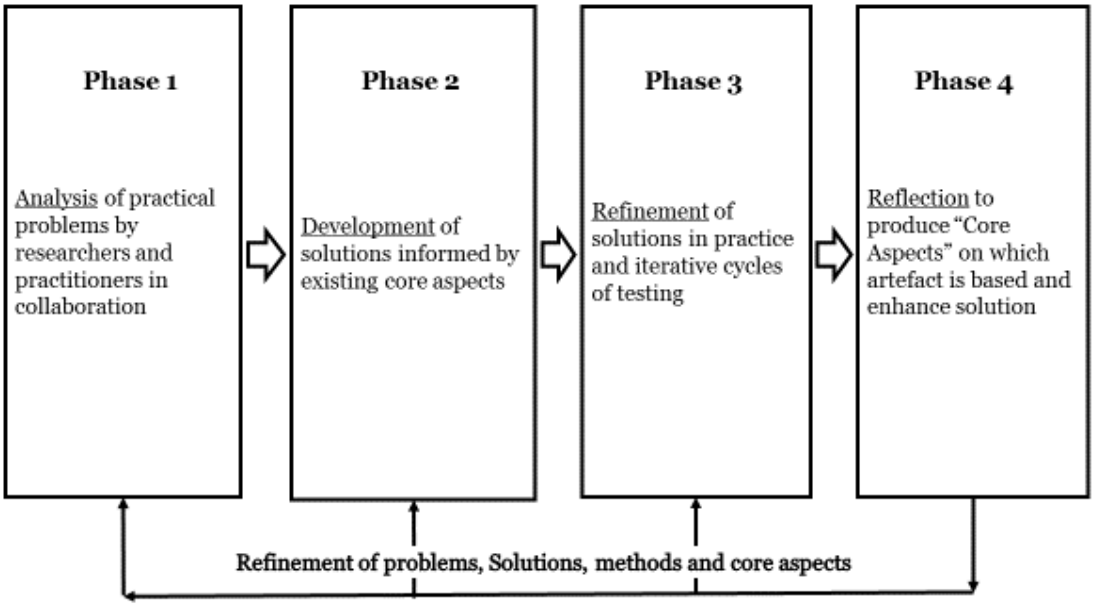

Figure 4.2: Design-based research (Herrington et al., 2007)

Table 4.1: Design-based approach phases (Herrington et al, 2007)

No	Phase	Element
1	Analysis of practical problems by researchers and stakeholders in collaboration	Statement of problem Consultation with researchers and stakeholders Research objectives Literature Review
2	Development of solutions informed by existing core aspects and technological innovations	Theoretical framework Development of theoretical core aspects to guide the design of the intervention Description of proposed intervention
3	Iterative cycles of testing and refinement of solutions in practice	Implementation of intervention (First iteration) Participants Data collection Data analysis Implementation of intervention
		Second and further iterations Participants Data collection Data analysis
4	Reflection on core aspects of produced artefact and enhanced solution implementation	Design principles Designed artefact(s) Professional development

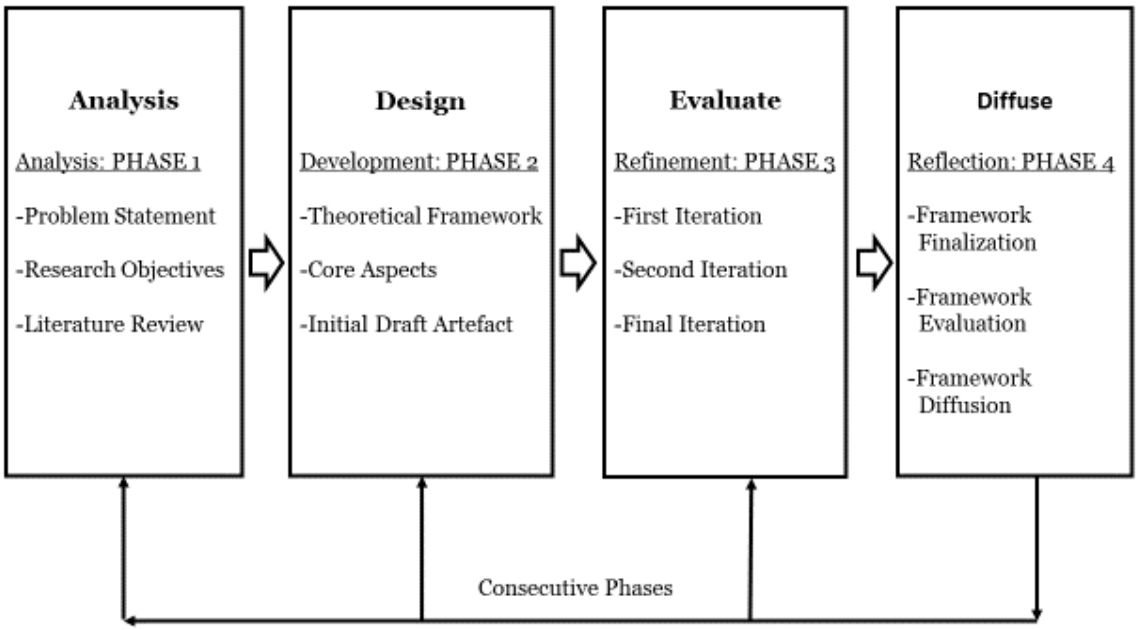

Figure 4.3: Nelson Mandela University-Design Science Framework Methodology (NMU-DSFM)

To contextualise NMU-DSFM depicted in Figure 4.3, each phase will be analysed. In Phase 1 according to Herrington et al. (2007), the researcher analyses the practical problem and this analysis resulted in the formulation of problem statement followed by research objectives. Furthermore, Phase 1 requires the researcher to conduct a literature review. Upon the completion of the literature review, the final refined problem statement is presented, and secondly, it presents unique objectives that have been identified that will address the problem at hand.

Phase 2 describes the solution to the problem identified in Phase 1 according to Herrington et al., (2007). This phase requires that the researcher conducts study of literature in order to identify core aspects that are typically required in the state-of-the-art Framework for implementation of Awareness, Education and Training (F-CSAET). It also requires the researcher to address the 'Theoretical Framework' elements. This is done through analysis of literature as this is the basis for developing a state-of-the art F-CSAET. The output of Phase 2 is an initial theoretical of F-CSAET, which aims to contribute to the real-world problem.

As described by Herrington et al., (2007), Phase 3 requires the researcher to refine state-of-the art F-CSAET through analysis of the gap between benchmark CSAET and current employee-awareness levels. This is to ensure that the final F-CSAET is tailored to solve

the organisation's real challenges. Current employee-awareness levels are determined through application of Human Aspects of Information Security-Questionnaire (HAIS-Q). The first literature based F-CSAET is tested for acceptance with the stakeholders. The feedback is then incorporated into a second F-CSAET. After incorporating the feedback, the improved F-CSAET follows further evaluation as the first F-CSAET. The iterative cycles will continue until F-CSAET reaches an acceptable level, as determined by the relevant stakeholders within LEDA Group (Osterle et al., 2010). The output of Phase 3 is the final F-CSAET.

Herrington et al. (2007) describes phase 4 as a reflection on core aspects of produced framework and enhancement of solution implementation. On this phase, a comparison of the benchmark F-CSAET are compared with the tailored F-CSAET to ensure compliance with core aspects assessment, plan, train and reinforce as outlined in the state-of-the art F-CSAET in chapter 3. The output of this phase is the final artefact (F-CSAET) and its release to stakeholders, and publishing of the solution.

4.3 Research Methods

The steps followed to implement phases of NMU-DSFM are discussed in this section. Chapter 1 defined the problem statement developed primary and secondary objectives. The problem statement and the research objectives were refined through a literature review. In this research LEDA Group was used as a case study (Yin, 2013). The primary objective of the research was determined to be the development of a framework to direct and implement cybersecurity awareness, education and training with the LEDA Group. The achievement of the secondary objectives serves as stepping stones towards achieving the primary objective. Chapter 2 and 3 reports on a literature review. Potential cybersecurity threats and attacks and cybersecurity reports from various players in the industry were analysed. The role of employees/ human beings in prevention of cybersecurity was identified through literature review. The core knowledge of the ideal CSAET was identified. Chapter 2 and 3 met requirements of Phase 1 of the NMU-DSFM.

Phase 2 of the NMU-DSFM presents the development of the theoretical framework based on the literature review. Chapter 3 identified the four steps as the phases of the theoretical framework. The four steps in Figure 3.1 were discussed in Chapter 3 and formed core aspects of the theoretical framework, Figure 3.1. The theoretical framework is refined in phase 3 (evaluate) of the NMU-DSFM. The theoretical framework will be

refined in Chapter 6 taking in to account the analysis of data collected and analysed in Chapter 5.

To determine the refinement required, it is necessary to collect data from LEDA Group employees. To collect data and produce analysis results with integrity, objectivity, reliability and relevance, the Human Aspects of Information Security-Questionnaire (HAIS-Q) (Parsons et al., 2013, 2014, & 2017) was utilised in this research. HAIS-Q was developed for the purpose of evaluating information security threats caused by employees within organisations (Parsons et al, 2013). The instrument has been developed and refined using a variety of populations, including students, the general public, and employees from government and financial institutions in Australia (Parsons et al., 2017).

The HAIS-Q provided an appropriate tool to collect data to determine the level cybersecurity awareness of employees. This was so because the HAIS-Q focuses on seven areas identified in chapter 2 and 3. HAIS-Q enabled us to collect data regarding knowledge, attitude and behaviour of employees when using computer for work (Parsons et al., 2017). The data collected was analysed to establish the gap between the benchmark cybersecurity awareness level and the current level.

The data was collected from employees at the start of evaluate phase. The survey questions are electronically send to employees using on-line survey facility called QuestionPro. The objective of data collection was to achieve one of the secondary objectives, to determine the level of the cybersecurity awareness of the LEDA Group employees. The gap between the current level and the benchmark level identified through literature review in Chapter 3 will be analysed. The analysis forms the pillar of the refinement of the theoretical F-CSAET. The other essential role is played by Cybersecurity Interest Team (CIT) formed by members of the IT Governance Committee of the LEDA Group, members of the IT division and IT Audit Specialist within the LEDA Group. The theoretical F-CSAET will be refined based on the analyses of the gap and the input of the CIT until a final F-CSAET is produced. The input of the CIT will be discussed in Chapter 6.

The objective of this research is to develop F-SAET. F-CSAET aims at guiding CSAET efforts in the provision of the appropriate knowledge to change the attitude of the employees in order to change their behaviour towards cybersecurity. The HAIS-Q asks

three sets of questions, (1) your knowledge of computer use guidelines, (2) your attitude towards these computer use guidelines, (3) your behaviour when using a computer for work. Sixty three (63) questions were asked. Respondents are required to respond on a Likert-type scale, ranging from Strongly Disagree to Strongly Agree.

In order to achieve the secondary objectives of the research, inductive reasoning approach will be followed (Hayes, Heit & Swendsen, 2010). The observations and analyses of the responses by the survey LEDA Group employees regarding knowledge, attitude and behaviour will be used to make conclusions about the level of knowledge of cybersecurity. The responses will measured against best knowledge, attitude and behaviour in Table 2.6 and best response for each question. Reverse scoring will be used for negative questions. Mean analysis including one-way variance analysis will be performed and will form the basis of our inductive reasoning (Kaufmann & Schering, 2014). The scores between 3 and 3.9 are rated as middle of the ground which means undecided.

The diffusion phase was performed through the CIT. The CIT will evaluate the F-CSAET for Abstraction which means artefact must be applicable to a class of problems in order to ensure real contribution by the research, Originality meaning artefact must substantially contribute to the advancement of the body of knowledge, Justification which means artefact must be justified in a comprehensible manner and must allow for its validation and Benefit which means artefact must yield benefit – either immediately or in the future – for the respective stakeholder groups.

4.4 Conclusion

In this chapter, NMU-DSFM was identified as the primary research method. This research method will be utilised to research the level of cybersecurity awareness and the development of the cybersecurity awareness framework. The objective of the framework is to improve level found through research to the benchmark discussed in Chapter 3 (Osterle et al., 2010). The NMU-DSFM is a combination of Design-Oriented Information Systems Research and Design-based Research methodologies.

Design-oriented research approach provides the researcher with academic freedom in choosing methods to follow during the research. Design-based approach provides the researcher with comprehensive guidelines to complement design-oriented approach

(Herrington et al, 2007). NMU-DSFM is suitable enable the achievement of the primary objective of this research as identified in Chapter 1.

In applying NMU–DSFM in Chapter 5, Human Aspects of Information Security-Questionnaire (HAIS-Q) was utilised to collect data from LEDA Group employees (Parsons et al., 2013, 2014 & 2017). The employees were asked sixty three (63) questions using Likert scale. The results will be analysed to establish the gap between the benchmark and the actual level of cybersecurity awareness. This analysis was used to tailor a LEDA framework for implementation of cybersecurity awareness, education and training.

CHAPTER 5: DATA COLLECTION AND ANALYSIS

Research methodology and methods identified in Chapter 4 were applied in this chapter to achieve the research objectives. The Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons et al., 2017) was selected as the vehicle to collect the data from the LEDA Group employees. The survey with HAIS-Q was randomly sent to employees using the QuestionPro on-line facility. The limitation of the HAIS-Q is the fact that it is a self-report measure (Parsons et al., 2014). The respondents may be bias due to factors such as fear of punishment, dispositional characteristics, true state of affairs in cases of violation, sensitivity of the subject, etc. Further studies to establish validity of HAIS-Q however produced scientific evidence to confirm validity of HAIS-Q as a measure of information security awareness (Parsons et al., 2017).

This chapter discusses the survey and presents the results. The results provide insights to the current level of knowledge, attitude and behaviour of the LEDA Group employees towards cybersecurity. Specifically, the chapter highlights the gap within the benchmark level determined in Chapter 3. Understanding the gap will assist to focus the development of FCSAET. The collection and analysis of data focussed on the seven knowledge units identified in Chapter 2. One-way analysis of variance (ANOVA) was used to determine whether there were any statistically significant differences between the means of the groups.

5.1 Survey and validity

The Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons et al., 2017) was applied in the form of a questionnaire. According to Parsons et al., (2017), the questionnaire was validated in two further studies in which 112 and 505 respondents respectively participated. The results of a factor analysis and other statistical techniques provided evidence for the validity of the HAIS-Q as a robust measure of ISA (Parsons et al., 2017). The results proved that the HAIS-Q can predict an aspect of cybersecurity behaviour, and provides evidence for its convergent validity (Parsons et al., 2017).

Participants were instructed to respond to each item on a five-point Likert scale from Strongly Disagree to Strongly Agree. An on-line survey was randomly sent to more than 400 employees within the LEDA Group. Of the employees, 314 viewed the survey; 184 started responding to the questions; and 137 completed all the questions in the survey.

The 184 respondents included executive managers, senior managers, junior managers and other officials. Participants included officials between the ages of 19 and 65 years of age, 81 females and 56 males. Almost 95% of the participants confirmed having spent between 3 and 8 hours on a computer or mobile devices on a daily basis. Some participants confirmed having received the emails on laptop, cellphone and iPad.

5.2 Mean between KAB and ANOVA calculation

One-way analysis of variance (ANOVA) is used to determine whether there are any statistically significant differences between the means of three or more independent groups (Kim, 2014). ANOVA calculations were performed to determine if the means in Table 5.1, among knowledge, attitude and behaviour were equal or different. ANOVA analysis follows the hypothesis that H_o: $\mu_K = \mu_A = \mu_B$, where H_o is null hypothesis, μ_K is mean for knowledge, μ_A is mean for attitude and μ_B is mean for behaviour. The relationship among knowledge, attitude and behaviour is in that the knowledge that a person has about cybersecurity policies, procedures and practices influences the person's attitude about cybersecurity issues which in turn determines the behaviour of the person when confronted with cybersecurity challenges (Parsons et al, 2014).

Table 5.1: Comparison – KAB elements

Focus area	Mean		
	Knowledge	Attitude	Behaviour
Password Management	4.41	4.19	4.00
Email use	3.82	3.87	4.00
Internet use	2.94	3.88	3.47
Social media	4.18	4.12	4.11
Mobile devices	4.38	4.30	4.58
Information handling	4.33	4.56	4.45
Incident reporting	4.01	4.16	4.05

The comparison of the means per focus area show that where there is knowledge, the attitude and the behaviour become positive, except for email use and Internet use.

In the case of email use and Internet use, the mean for knowledge is lower but for attitude and behaviour the mean is higher signifying good attitude and behaviour.

This observation required the performance of ANOVA in Table 5.2 to determine whether there was a significant difference among the means. The ANOVA was performed at significant level (α) = 0.05.

The results of ANOVA show that for employees of the LEDA Group, the level of knowledge, attitude and behaviour for password management was directly proportional to one another. This means that when employees have the appropriate level of knowledge they tend to have good cybersecurity attitude and behaviour. In cases where their attitude and behaviour were not appropriate, training and educating them would result in a change in attitude and behaviour. The CSAET programme relating to password management should constantly ensure that appropriate password management knowledge is provided to employees. The attitude and behaviour should be assessed rigorously as the findings points to the knowledge gap that is required to change the attitude and behaviour.

The ANOVA results for email use, Internet use, social media, mobile devices, information handling and incident reporting show similar patterns as for password management. The cybersecurity knowledge level is directly proportional to attitude and behaviour from the analysis in Table 5.2, $\mu_K = \mu_A = \mu_B$ for each set of KAB for all seven focus areas. This means that the knowledge level for cybersecurity brings corresponding good attitude and behaviour.

Overall, the results of the ANOVA test on the data collected from the LEDA Group employees show that the attitude and behaviour of employees is dependent on the cybersecurity knowledge they have. This observation provides the LEDA Group with a real opportunity to convert the employees into strongest link when coming to the prevention of cybersecurity breaches. Appropriate assessment and analysis of cybersecurity attitude and behaviour is confirmed by the ANOVA test results to be key in identifying the relevant knowledge gap. The knowledge gap informs the content of CSAET programme.

Table 5.2: ANOVA results and conclusions at α = 0.05 significance level

SS		df	MS	F	F(critical)	F vs F(critical)	Conclusion
Password Management							
Between	0.081	2	0.037				
Within	0.527	6	0.088	0.418	5.14	F < F(critical)	$H_{o\ holds}$
Total	0.600	8					
Email use							
Between	0.145	2	0.059				
Within	1.229	6	0.205	0.288	5.14	F < F(critical)	$H_{o\ holds}$
Total	1.346	8					
Internet use							
Between	1.336	2	0.668				
Within	1.732	6	0.289	2.312	5.14	F < F(critical)	$H_{o\ holds}$
Total	3.070	8					
Social media							
Between	0.009	2	0.004				
Within	1.431	6	0.239	0.018	5.14	F < F(critical)	$H_{o\ holds}$
Total	1.440	8					
Mobile devices							
Between	0.129	2	0.064				
Within	0.492	6	0.082	0.785	5.14	F < F(critical)	$H_{o\ holds}$
Total	0.621	8					
Information handling							
Between	0.079	2	0.040				
Within	0.390	6	0.065	0.611	5.14	F < F(critical)	$H_{o\ holds}$
Total	0.470	8					
Incident reporting							
Between	0.035	2	0.018				
Within	0.360	6	0.060	0.292	5.14	F < F(critical)	$H_{o\ holds}$
Total	0.395	8					

5.3 Results and discussion

Reverse scoring was used on some items marked with an asterisk as shown in Tables 5.1 to 5.7. The mean, as shown in Tables 5.1 to 5.7, is used to analyse Knowledge, Attitude and Behaviour (KAB) for each focus area. A mean of 1 meant more insecure KAB, while 3 was the middle ground and 5 meant more secure KAB. Three aspects for each focus area were tested for knowledge, attitude and behaviour and the results are expressed in terms of the mean as illustrated in Tables 5.1 to 5.8 and graphs in Figures 5.1 to 5.7. Results for KAB are discussed for each area.

5.3.1 Password management

The mean for password management knowledge was 4.41. This shown good knowledge regarding the use of the same passwords, sharing of passwords, and strong passwords. There were, however, 12% of the respondents who ranged from more insecure to undecided regarding the use of same passwords between work and social media accounts; 6% regarding the sharing of passwords with colleagues; and 13% regarding the choice of strong passwords.

The mean for password management attitude was 4.19. This shown good attitude regarding the use of the different passwords between work and social media accounts, not sharing of passwords, and the use of strong passwords. There were, however, 5% of the respondents who ranged from more insecure to undecided regarding the use of different passwords between work and social media accounts; 24% regarding sharing of passwords; and 13% regarding the use of strong passwords.

On the other hand, the mean for password management behaviour was 4.31. This shown good behaviour regarding the management of passwords. There were, however, 14% of the respondents who ranged from more insecure to undecided regarding the use of the different passwords between work and social media accounts; 4% regarding the sharing of passwords; and 10% regarding the use of strong passwords.

Based on the analysis of the survey results, the confidentiality and integrity of the information asset was vulnerable. This was due to potential unauthorised access to information as a result of a small number of officials who may use the same passwords for work and social media accounts, may share passwords with colleagues, and use weak

passwords. CSAET within the LEDA Group should include password management targeting this group while reinforcing knowledge, good attitude and good behaviour for the rest of the officials. The CSAET programme should seek to identify the vulnerable group through appropriate awareness assessment.

Table 5.3: Password management – KAB mean analysis

Password Management	**Knowledge item**	**Mean**
Using the same password	It is acceptable to use my social media passwords on my work accounts*	4.45
Sharing passwords	I am allowed to share my work passwords with colleagues*	4.63
Using a strong passwords	A mixture of letters, numbers and symbol is necessary for work passwords	4.14
Mean		**4.41**
Password Management	**Attitude item**	**Mean**
Using the same password	It is safe to use the same password for social media and work accounts*	4.53
Sharing passwords	It's a bad idea to share my work passwords, even if a colleague asks for it	3.76
Using a strong passwords	It is safe to have a work password with just letters*	4.27
Mean		**4.19**
Password Management	**Behaviour item**	**Mean**
Using the same password	I use a different a different passwords for my social media and work accounts	4.17
Sharing passwords	I share my work passwords with colleagues*	4.57
Using a strong passwords	I use a combination of letters, numbers and symbols in my work passwords	4.21
Mean		**4.32**
Focus area mean		**4.31**

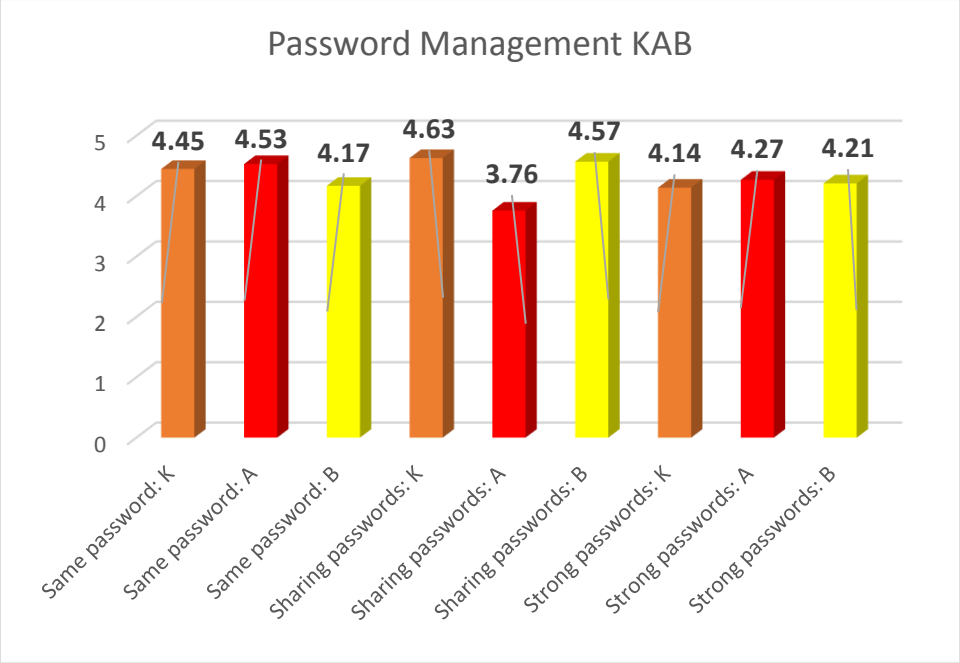

Figure 5.1: Password management mean analysis

Figure 5.1 shows that although employees had good knowledge regarding password sharing, there was susceptibility for sharing passwords. This could be attributed to factors such as trust of colleagues, not understanding why passwords should not be shared or commitment to work and therefore believing that not sharing a password may impact negatively on work progress. The CSAET programme for the LEDA Group should target the attitude gap. The programme should educate the employees on why passwords should not be shared and should articulate the risks of sharing passwords to both employees and the LEDA Group's information asset. The analysis concludes that while knowledge appears good on the results, it was not adequate to change the attitude of the employees. There was a knowledge gap pointed to by the employee attitude.

5.3.2 Email use

The mean for email use knowledge was 3.82. This shown 'middle of the road' knowledge regarding clicking on links in emails from known senders, clicking on links in emails from unknown senders and opening attachment in emails from unknown senders. There were however 38% of respondents who ranged from more insecure to undecided regarding clicking on links in emails from known senders, 36% regarding clicking on links in emails from unknown senders and 12% regarding opening attachment in emails from unknown senders.

The mean for email use attitude was 3.87. This shown 'middle of the road' attitude regarding clicking on links in emails from known senders, clicking on links in emails from unknown senders and opening attachment in emails from unknown senders. There were however 47% of respondents who ranged from more insecure to undecided regarding clicking on links in emails from known senders, 7% regarding clicking on links in emails from unknown senders and 23% regarding opening attachment in emails from unknown senders.

On the other hand, the mean for email use behaviour was 4.00. This shown good behaviour regarding email use. There were however 17% of respondents who ranged from more insecure to undecided regarding clicking on links in emails from known senders, 11% regarding clicking on links in emails from unknown senders and 25% regarding opening attachment in emails from unknown senders.

Based on the analysis of the survey results, officials are likely to open links and attachments that appear to be from known sender. With 47% believing that it is always safe to click on links in emails from people they know, the risk of clicking on links in the socially engineered email is high. The results shown that the officials were vulnerable to both spear phishing and phishing emails as the sender tries smart to make it appear legitimate. LEDA Group therefore is exposed to social engineering and phishing attacks. CSAET should enable officials to spot a phishing email. The CSAET programme should include practical testing of knowledge by sending fake phishing emails.

Table 5.4: Email use – KAB mean analysis

Email use	Knowledge item	Mean
Clicking on links in emails from known senders	I am allowed to click on any links in emails from people I know*	3.66
Clicking on links in emails from unknown senders	I am not permitted to click on a link in an email from unknown sender	3.50
Opening attachment in emails from unknown senders	I am allowed to open email attachments from unknown senders*	4.29
Mean		**3.82**
Email use	**Attitude item**	**Mean**
Clicking on links in entails from known senders	It is always safe to click on links in emails from people I know*	3.31
Clicking on links in emails from unknown senders	Nothing bad can happen if I click on a link in an email from an unknown sender*	4.45
Opening attachment in emails from unknown senders	It is risky to open an email attachment from an unknown sender	3.85
Mean		**3.87**
Email use	**Behaviour item**	**Mean**
Clicking on links in entails from known senders	I do not always click on links in emails just because they come from someone I know	3.90
Clicking on links in emails from unknown senders	If an email from an unknown sender looks interesting, I click on a link within it*	4.22
Opening attachment in emails from unknown senders	I do not open email attachment if the sender is unknown to me	3.87
Mean		**4.00**
Focus area mean		**3.90**

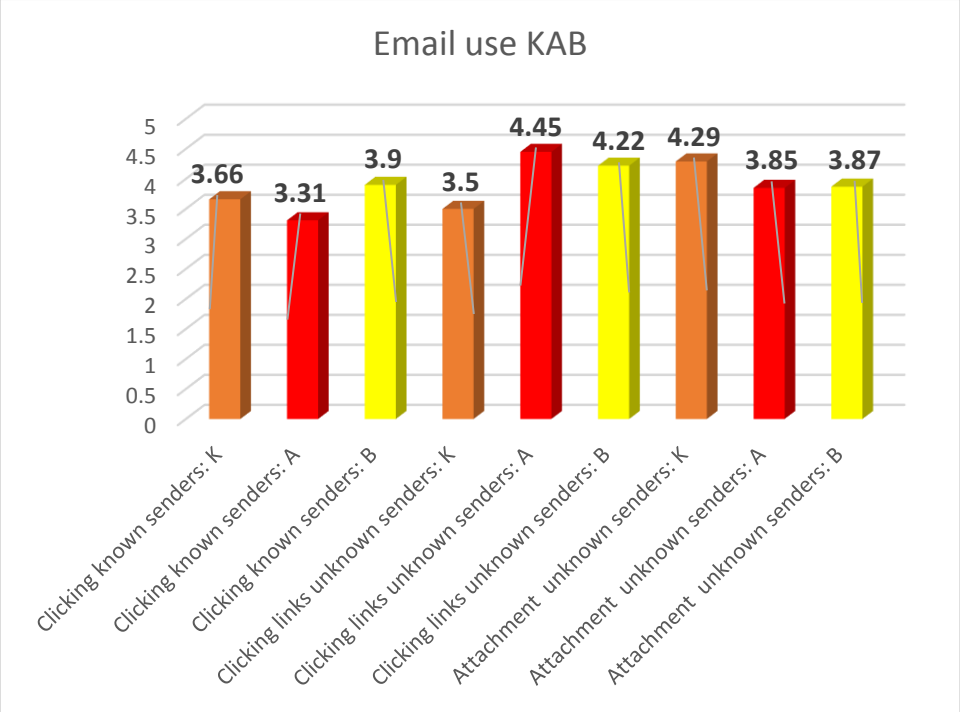

Figure 5.2: Email use mean analysis

Figure 5.2 shows susceptible knowledge, attitude and behaviour on clicking on email links from both known and unknown senders, and opening email attachments from the LEDA Group employees. Although the attitude for clicking on links of emails from unknown senders appears to be good, it is not convincing as knowledge about the same aspect is found to be suspect. This good attitude may be attributed to factors such as common sense by the respondents to the questionnaire. It is a good cybersecurity position by the LEDA Group to include the KAB of email use in the CSAET. The KAB of the employees is not adequate to seriously counter or prevent phishing and social engineering attacks. The sophistication of phishers and social engineers is likely to appear and trusted as known senders by employees. The CSAET should cover, among others, recognition of phishing and social engineering emails as these specifically aim to deceive the recipient into believing it is from a known sender and therefore legitimate.

5.3.3 Internet use

The mean for Internet use knowledge was 2.94. This shown inadequate knowledge regarding downloading of files from Internet, accessing dubious websites and entering information on line. 72% of respondents ranged from more insecure to undecided

regarding downloading of files from Internet, 37% regarding accessing dubious websites and 61% regarding entering information on line.

The mean for Internet use attitude was 3.88. This shown 'middle of the road' attitude regarding downloading of files from Internet, accessing dubious websites. There were however 12% of respondents who ranged from more insecure to undecided regarding downloading of files from Internet, 22% regarding accessing dubious websites and 26% regarding entering information on line.

On the other hand, the mean for Internet use behaviour was 3.47. This shown 'middle of the road' regarding Internet use. There were however 66% of respondents who ranged from more insecure to undecided regarding downloading of files from Internet, 25% regarding accessing dubious websites and 23% regarding entering information on line.

Based on the analysis of the survey results, the officials did not have the adequate knowledge, best attitude and best behaviour regarding the use of Internet. This exposed LEDA Group to attacks such as virus and malware. These attacks threatens availability of information asset and adversely impact business continuity. The CSAET program should thoroughly cover the knowledge, attitude and behaviour aspects of Internet use. The education and training should be continuous in order to reinforce the learning (Pashler et al., 2007).

Table 5.5: Internet use – KAB mean analysis

Internet use	Knowledge item	Mean
Downloading files	I am allowed to download any files onto my work computer if they help me to do my job*	2.44
Accessing dubious websites	While I am at work, I shouldn't access certain websites	3.49
Entering information on line	I am allowed to enter any information on any website if it helps me do my job*	2.90
Mean		**2.94**
Internet use	**Attitude item**	**Mean**
Downloading files	It can be risky to downloading files on my work computer	3.74
Accessing dubious websites	Just because I can access a website at work, does not mean that it is safe	4.06
Entering information online	If it helps me to do my job, it does not matter what information I put on a website*	3.85
Mean		**3.88**
Internet use	**Behaviour item**	**Mean**
Downloading files	I download any files onto my work computer that will help me get the job*	2.62
Accessing dubious websites	When accessing the Internet at work, I visit any website that I want to*	3.91
Entering information online	I assess the safety of the websites before entering information	3.93
Mean		**3.47**
Focus area mean		**3.43**

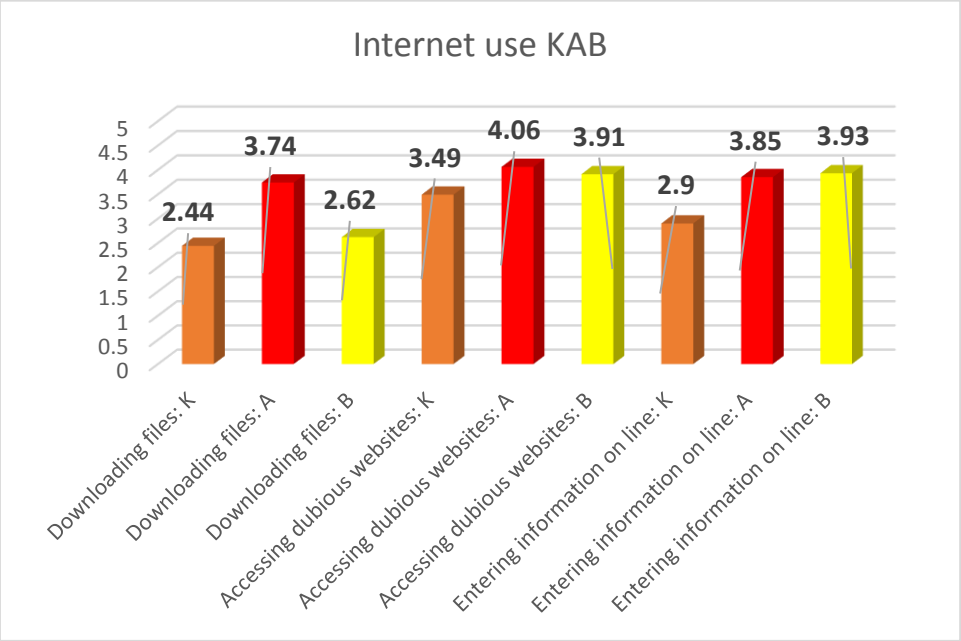

Figure 5.3: Internet use mean analysis

Figure 5.2 shows susceptible knowledge, attitude and behaviour on downloading files, accessing dubious websites and entering information on line in the LEDA Group employees. Although the attitude for accessing dubious websites appear to be good, it is not convincing as knowledge on the same aspect is found to be susceptible. The good attitude may be attributed to factors such as common sense by the respondents to the questionnaire. It is good cybersecurity position by the LEDA Group to include the KAB of Internet use in CSAET. Both KAB of the employees is not adequate to seriously counter and prevent hacking and virus attacks. The hackers need dots to connect and ultimately gain access to information network and system. Connecting to the Internet with no adequate understanding of risks involved could open up the LEDA Group to hacking and virus attacks. The cost of recovering from service denial and hacking incidents is much greater than preventing such incidents through proper CSAET.

5.3.4 Social media

The mean for social media use knowledge was 4.18. This shown good knowledge regarding the use of social media privacy settings, consideration of consequences and posting about work. There were, however, 25% of the respondents who ranged from

more insecure to undecided regarding the use of social media privacy setting; 21% regarding the consideration of consequences; and 2% regarding posting about work.

The mean for social media use attitude was 4.12. This shown good attitude regarding social media privacy settings, consideration of consequences and posting about work. There were, however, 25% of the respondents who ranged from more insecure to undecided regarding social media privacy settings; 9% regarding consideration of consequences, and 15% regarding posting about work.

On the other hand, the mean for social media use behaviour was 4.11. This shown good behaviour regarding the use of social media. There were, however, 39% of the respondents who ranged from more insecure to undecided regarding social media privacy settings, 9% regarding consideration of consequences, and 1% regarding posting about work.

Based on the analysis of the results of the survey, there is likely risk posed by social media privacy settings. Hackers could obtain links to work accounts through social media use and behaviour of the officials owing to vulnerabilities around social media privacy settings. The impact of this risk is high and costly; therefore, the CSAET programme should address awareness and education regarding this aspect of social media use. The programme should answer why one must periodically review the privacy settings on social media accounts. This should be reinforced to convert the review of privacy settings on social media accounts into culture.

Table 5.6: Social media use – KAB mean analysis

Social media use	Knowledge item	Mean
Social Media privacy settings	I must periodically review the privacy setting on social media accounts	3.75
Considering consequences	I cannot be fired for something I post on social media*	4.10
Posting about work	I can post what I want about work on social media*	4.69
Mean		**4.18**
Social media use	**Attitude item**	**Mean**
SM privacy settings	It is a good idea to regularly review my social media privacy settings	3.73
Considering consequences	It does not matter if I post things on social media that I would not normally say in public*	4.42
Posting about work	It is risky to post certain information about my work on social media	4.20
Mean		**4.12**
Social media use	**Behaviour item**	**Mean**
SM privacy settings	I do not regularly review my social media privacy settings*	3.47
Considering consequences	I do not post anything on social media before considering any negative consequences	4.20
Posting about work	I post whatever I want about my work on social media*	4.67
Mean		**4.11**
Focus area mean		**4.14**

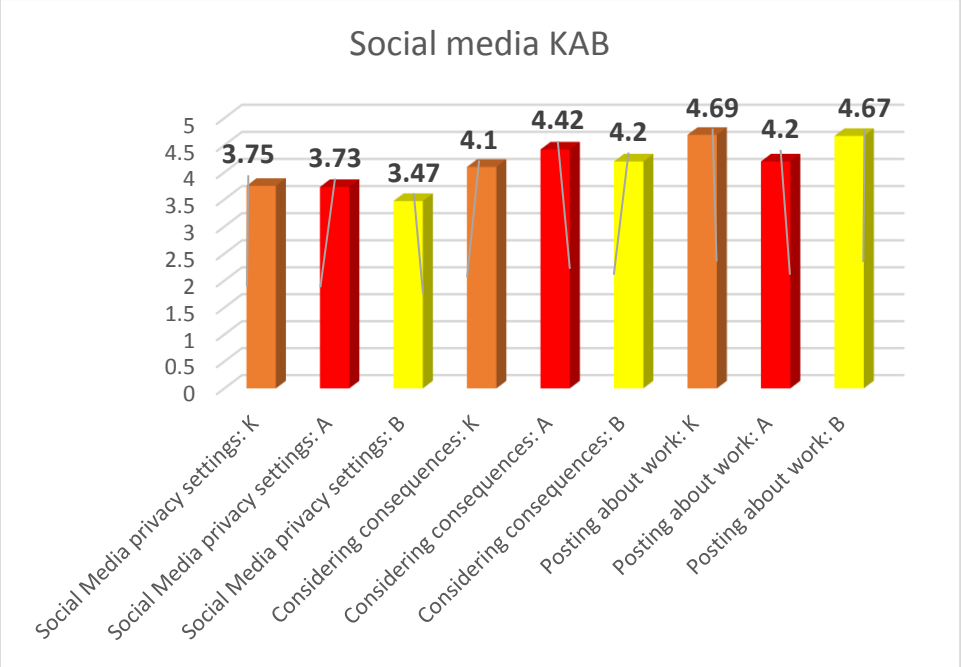

Figure 5.4: Social media use mean analysis

Figure 5.4 shows knowledge levels regarding social media privacy settings. These results point to the exposure the LEDA Group has as far as exposing the information to cyber risks through private interaction with cyber space. The LEDA Group CSAET should uplift the appropriate knowledge and educate the employees as to why social media privacy settings are critical to cybersecurity for the company. The KAB regarding consideration of consequences about posting and posting about work on social media is high. It is, however, a good cybersecurity position for the LEDA Group to keep constant CSAET over this area as these results might have marginal errors.

5.3.5 Mobile devices

The mean for mobile device use knowledge was 4.38. This shown good knowledge regarding physically securing mobile devices, sending sensitive information via Wi-Fi and shoulder surfing. There were, however, 18% of the respondents who ranged from more insecure to undecided regarding physically securing mobile devices; 16% regarding sending sensitive information via Wi-Fi; and 4% regarding shoulder surfing.

The mean for mobile device attitude was 4.30. This shown good attitude regarding physically securing mobile devices, sending sensitive information via Wi-Fi and shoulder surfing. There were, however, 2% of the respondents who ranged from more

insecure to undecided regarding physically securing mobile devices, 24% regarding sending sensitive information via Wi-Fi, and 10% regarding shoulder surfing.

On the other hand, the mean for mobile device behaviour was 4.58. This shown good behaviour regarding mobile devices. There were, however, 3% of respondents who ranged from more insecure to undecided regarding physically securing mobile devices, 6% regarding sending sensitive information via Wi-Fi, and 5% regarding shoulder surfing.

Based on the analysis of the survey, the use of public Wi-Fi may be a source of risk to information asset. This has an adverse impact on the confidentiality of the LEDA Group information. The CSAET programme should identify officials who are most likely working with sensitive information and should educate them on the aspects of sensitive information and the use of public Wi-Fi. The programme should include identification and differentiation of sensitive information.

Table 5.7: Mobile devices – KAB mean analysis

Mobile devices	**Knowledge item**	**Mean**
Physically securing mobile devices	When working in a public place, I have to keep my laptop with me at all times	4.23
Sending sensitive information via Wi-Fi	I am allowed to send sensitive work files via a public Wi-Fi network*	4.31
Shoulder surfing	When working on sensitive documents, I must ensure that strangers cannot see my laptop screen	4.59
Mean		**4.38**
Mobile devices	**Attitude item**	**Mean**
Physically securing mobile devices	When working at café, it is safe to leave my laptop unattended for a minute*	4.75
Sending sensitive information via Wi-Fi	It is risky to send sensitive work files using a public Wi-Fi network	3.89
Shoulder surfing	It is risky to access sensitive work files on laptop if strangers can see my screen	4.26
Mean		**4.30**
Mobile devices	**Behaviour item**	**Mean**
Physically securing mobile devices	When working in a public place, I leave my laptop unattended*	4.73
Sending sensitive information via Wi-Fi	I send sensitive work files using a public Wi-Fi network*	4.60
Shoulder surfing	I check that strangers cannot see my laptop screen if I am working on a sensitive document	4.42
Mean		**4.58**
Focus area mean		**4.42**

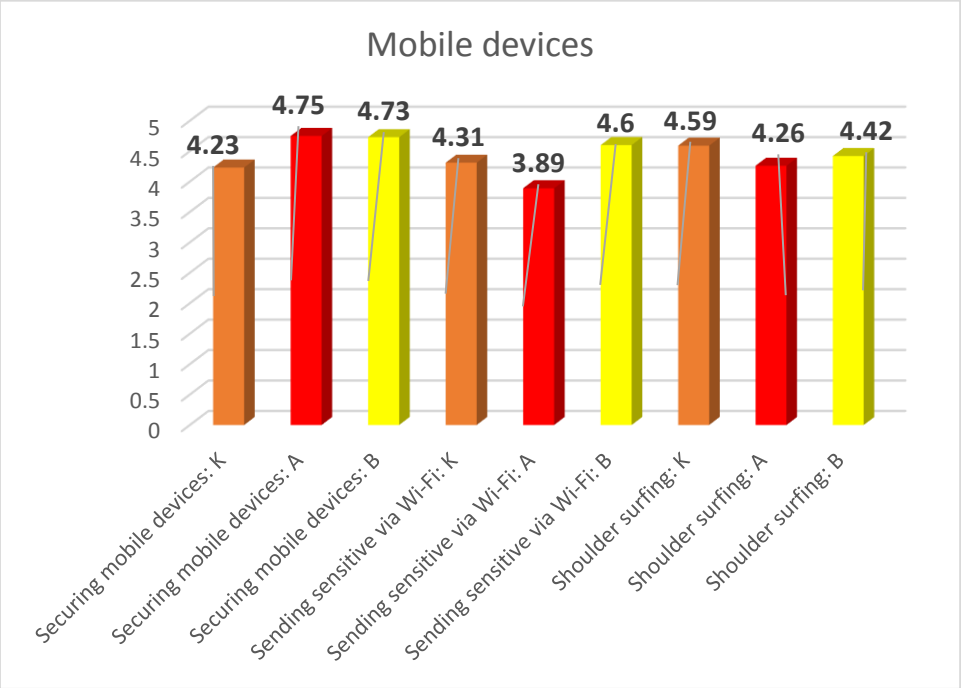

Figure 5.5: Mobile devices mean analysis

Figure 5.5 shows susceptibility of sending sensitive information via Wi-Fi. The LEDA Group CSAET should include education on the aspect of sending sensitive information via Wi-Fi. While the other KAB regarding mobile devices show good results, the LEDA Group should reinforce the good cybersecurity KAB over them. The reinforcement will also address the errors if they exist in the current results. The current results show an opportunity for errors in that employees have common sense in knowing that mobile devices are assets which should be secure and that shoulder surfing should be monitored at all times though they might not be practising such actions.

5.3.6 Information handling

The mean for information handling knowledge was 4.33. This shown good knowledge regarding the disposing of sensitive print-outs, inserting removable media and leaving sensitive material visible. There were, however, 6% of the respondents who ranged from more insecure to undecided regarding the disposing of sensitive print-outs, 25% regarding inserting removable media, and 3% regarding leaving sensitive material visible.

The mean for information handling attitude was 4.56. This shown good attitude regarding the disposing of sensitive print-outs, inserting removable media and leaving sensitive material visible. There were, however, 5% of the respondents who ranged from more insecure to undecided regarding the disposing of sensitive print-outs, 3% regarding inserting removable media, and 7% regarding leaving sensitive material visible

On the other hand, the mean for information handling behaviour was 4.45. This shown good behaviour regarding information handling. There were, however, 3% of the respondents who ranged from more insecure to undecided regarding the disposing of sensitive print-outs, 12% regarding inserting removable media, and 4% regarding leaving sensitive material visible.

Based on the analysis of the survey results, KAB of officials was at a secure level. There is, however, a concern relating to the inserting of removable media found in a public place. At 25%, it is likely that at least 27 officials would plug a USB stick found in a public place into their work computer. Since the adverse impact of this action on the information asset is high, CSAET should practically test this KAB by leaving appropriately programmed USB sticks in selected places, and reinforce the secure level found to push it up to a more secure level

Table 5.8: Information handling – KAB mean analysis

Information handling	Knowledge item	Mean
Disposing of sensitive print-outs	Sensitive Print-outs can be disposed of in the same way as non-sensitive ones*	4.53
Inserting removable media	If I find a USB stick in a public place, I should not plug it into my work computer	3.89
Leaving sensitive material visible	I am allowed to leave print-outs containing sensitive information on my desk overnight*	4.58
Mean		**4.33**
Information handling	**Attitude item**	**Mean**
Disposing of sensitive print-outs	Disposing of sensitive print-outs by putting them in the rubbish bin is safe*	4.58
Inserting removable media	If I find a USB stick in a public place, nothing bad can happen if I plug it into my work computer*	4.68
Leaving sensitive material visible	It is risky to leave print-outs that contain sensitive information on my desk overnight	4.43
Mean		**4.56**
Information handling	**Behaviour item**	**Mean**
Disposing of sensitive print-outs	When sensitive prints-outs need to be disposed of, I ensure that they are shredded or destroyed	4.57
Inserting removable media	I would not plug a USB stick found in a public place into my work computer	4.25
Leaving sensitive material visible	I leave print-outs that contain sensitive information on, my desk when I am not there*	4.54
Mean		**4.45**
Focus area mean		**4.45**

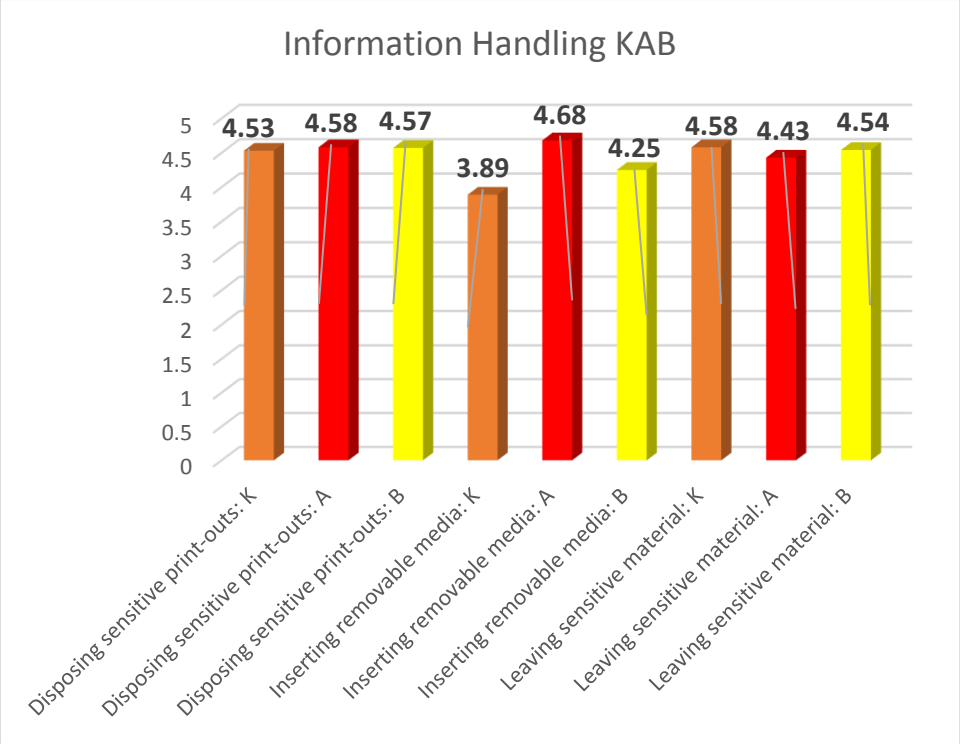

Figure 5.6: Information handling mean analysis

Figure 5.6 shows good knowledge, attitude and behaviour for disposing of sensitive print-outs, leaving sensitive information on a desk by the LEDA Group employees. It also shows susceptibility on the knowledge regarding the insertion of removable media onto computers/laptops or other devices. The susceptibility exposes the LEDA Group network to hacking risk. This aspect should be included in CSAET programme. The good attitude and behaviour shown on the results might be due to other factors such as common sense as it was found through the ANOVA test that attitude and behaviour are directly linked to knowledge.

5.3.7 Incident reporting

The mean for incident reporting knowledge was 4.01. This shown good knowledge regarding reporting suspicious behaviour, ignoring poor security behaviour by colleagues and reporting all incidents. There were, however, 10% of the respondents who ranged from more insecure to undecided regarding reporting suspicious behaviour, 16% regarding ignoring poor security behaviour by colleagues, and 25% regarding reporting all incidents.

The mean for incident reporting attitude was 4.16. This shown good attitude reporting suspicious behaviour, ignoring poor security behaviour by colleagues and reporting all incidents. There were, however, 6% of the respondents who ranged from more insecure to undecided regarding reporting suspicious behaviour, 9% regarding ignoring poor security behaviour by colleagues, and 17% regarding reporting all incidents.

On the other hand, the mean for incident reporting behaviour was 4.05. This shown good behaviour regarding incident reporting. There were, however, 12% of the respondents who ranged from more insecure to undecided regarding reporting suspicious behaviour, 29% regarding ignoring poor security behaviour by colleagues, and 6% regarding reporting all incidents.

Based on the analysis of the survey results, there was a likelihood that colleagues may not report other colleagues' poor security behaviour, and not report incidents. The CSAET should educate the officials in spotting and identifying an incident, and reinforce the secure level relating KAB of reporting suspicious behaviour, ignoring poor security behaviour by colleagues and reporting all incidents to push it into the more secure level.

Table 5.9: Incident reporting – KAB mean analysis

Incident reporting	**Knowledge item**	**Mean**
Reporting suspicious behaviour	If I see someone acting suspiciously in my workplace, I should report it	4.26
Ignoring poor security behaviour by colleagues	I must not ignore poor security behaviour by my colleagues	3.96
Reporting all incidents	It is optional to report security incidents*	3.81
Mean		**4.01**
Incident reporting	**Attitude item**	**Mean**
Reporting suspicious behaviour	If I ignore someone acting suspiciously in my workplace, nothing bad can happen*	4.35
Ignoring poor security behaviour by colleagues	Nothing bad can happen if I ignore poor security behaviour by a colleague*	4.21
Reporting all incidents	It is risky to ignore security incidents, even if I think they are not significant	3.91
Mean		**4.16**
Incident reporting	**Behaviour item**	**Mean**
Reporting suspicious behaviour	If I saw someone acting suspiciously in my workplace, I would do something about it	4.12
Ignoring poor security behaviour by colleagues	If I noticed my colleague ignoring security rules, I would not take any action*	3.74
Reporting all incidents	If I noticed a security incident, I would report it	4.28
Mean		**4.05**
Focus area mean		**4.07**

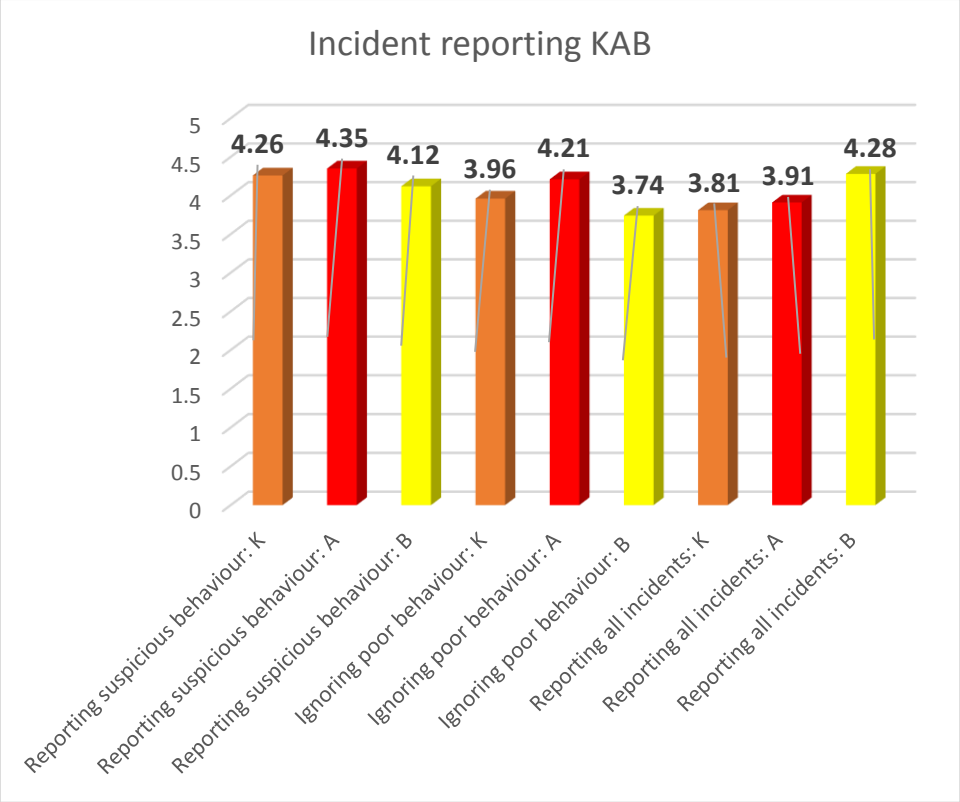

Figure 5.7: Incident reporting mean analysis

Figure 5.7 shows susceptibility to ignorance about poor security behaviour by colleagues on both knowledge and behaviour aspects, and on KAB of reporting all incidents. These areas of susceptibility should be included in the CSAET. The other areas showing good KAB should be on reinforcement in order to maintain the current awareness at benchmark level.

5.4 Conclusion

In this chapter, an analysis of the level of cybersecurity awareness was performed on the three aspects: knowledge, attitude and behaviour. These three aspects were analysed over seven focus areas, namely: password management, email use, Internet use, social media, mobile devices, information handling, and incident reporting. The objective of these analyses was to determine the level of awareness of officials regarding cybersecurity.

The areas of concern were cases in which the mean was below 3 or lying between 3 and 3.9. These areas were found in the attitude towards sharing passwords; knowledge towards clicking on links in emails from known senders, and clicking on links in emails from unknown senders; attitude towards clicking on links in emails from known

senders, and opening attachments in emails from unknown senders; behaviour towards clicking on links in emails from known senders, and opening attachments in emails from unknown senders; knowledge towards downloading files; accessing dubious websites, and entering information online; attitude towards downloading files and entering information on line; behaviour towards downloading files, accessing dubious websites, and entering information on line; knowledge, attitude and behaviour towards social media privacy settings; attitude towards sending sensitive information via Wi-Fi; knowledge towards inserting removable media; knowledge towards ignoring poor security behaviour by colleagues, and reporting all incidents; attitude towards reporting all incidents, and behaviour towards ignoring poor security behaviour by colleagues. Officials require differentiated CSAET on these areas of concern.

In order to implement CSAET, the LEDA Group requires a tailored F-CSAET informed by the data collected and analysed. Chapter 6 develops the F-CSAET and discusses the steps in the F-CSAET.

CHAPTER 6: DEVELOPMENT OF F-CSAET

The primary objective of this treatise was to develop a framework for the implementation of cybersecurity awareness, education and training. Both primary and secondary objectives were identified in Chapter 1. The ideal framework based on literature review was developed in Chapter 3. The four steps for the ideal framework were identified as assess, plan, implement, and reinforce.

Chapter 6 completes the process, which started with the ideal framework, of developing and tailoring the F-CSAET based on the case study, the LEDA Group. The ideal framework is refined with the input of the Cybersecurity Interest Team (CIT) and the feedback from analyses of the data collected from the LEDA Group employees. The final F-CSAET must meet the principles of abstraction, originality, justification and benefit. NMU-DSFM was followed from problem statement through development, refinement and finalisation of the F-CSAET. The aim of this Chapter is to move the theoretical F-CSAET to a real world solution for implementing CSAET using the case study. The successful implementation of the F-CSAET is dependent on Information Security Governance within the organisation.

6.1 Information Security Governance

Cybersecurity awareness, education and training is required to be directed by the Cybersecurity policy. The Cybersecurity policy should be directed by Information Security Governance within the organisation. There are best practices, which may be used as benchmarks for the content of the cybersecurity policy. These best practices include COBIT 5, ISO27001, ISO27005, ISO27008 and ISO27032, which support the implementation of ISO27001, and King IV. Best practices should always be used in concert as no best practice is fit for all environments in their entirety. A Cybersecurity policy should also take into account the requirements of compliance with legislation such as POPIA, the Copyright Act and bills such as the Cybersecurity Bill.

This governance aspect is key as it sets the tone at the top and is the foundation to ensure the Confidentiality, Integrity and Availability (CIA) of information within the Group. Information Security Governance is the shaper and builder of the cybersecurity culture within organisations (Da Veiga & Martins, 2017). The Group is increasingly becoming

dependent on IT for its business activities. Therefore, agile cybersecurity practices are a must. F-CSAET is one tool for Cybersecurity Governance to ensure CIA of information.

The governance component is generally static over time. F-CSAET should ensure compliance with applicable legislation. Legislation, such as POPIA and the Copyright Act, brings responsibility and accountability requirements regarding personal information, which is what is processed in the organisation, including in the case study. Employees should be aware not to infringe the copyrights of copyright owners. Non-compliance has a reputational risk. Chapter 2 identified the potential impact of cybersecurity risks. While the Cybersecurity Bill is not yet law in South Africa, its consideration adds more to readiness for compliance once it becomes law.

The Board of the LEDA Group should direct the Executive Management to develop a cybersecurity policy under the guidance of COBIT5, ISO27001, ISO27005, ISO27008, ISO27032, King IV and the constraints of POPIA and the Cybercrimes and Cybersecurity Bill. The Board should evaluate the policy, benchmark against the best practices, and approve an adequate policy. The Board should continually monitor the implementation and effectiveness of the cybersecurity policy.

Executive Management should apply King IV to develop the cybersecurity policy; apply ISO27001 and ISO27032 to identify what must be in the cybersecurity policy; apply COBIT5 to identify what the policy should direct; apply ISO27005 and ISO27008 to establish procedures for policy implementation; evaluate the cybersecurity policy and procedure for compliance with POPIA; and evaluate the cybersecurity policy for readiness to comply with the Cybercrimes and Cybersecurity Bill once it is signed into law.

6.1.1 ISO27001

The International Organization for Standardization (*ISO*) is an international standards-setting body composed of representatives from various national standards organisations. ISO27001, one of the standards set by ISO, provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system. The ISO27001 is a risk-based approach, which is technology-neutral, and defines the planning processes covering the definition of a security policy, the definition of the scope of the ISMS, the performance

of a risk assessment, the management of identified risks, the selection of control objectives and controls to be implemented, and the preparation of a statement of applicability (ISO/IEC, 2005). The Board of the LEDA Group can benchmark the cybersecurity policy against the guidance of ISO27001. Complying with ISO27001 inspires confidence in shareholders, clients, financiers, partners and others in the security of their information in possession of the LEDA Group.

6.1.2 Other ISO27000 (ISO27032, ISO27005 and ISO27008) series

The ISO27000 series provides best practice recommendations on information security management, and the management of information risks through information security controls. It covers, amongst others, privacy, confidentiality and cybersecurity issues. It is applicable to organisations of all shapes and sizes. All organisations are encouraged to assess their information risks, then to treat them using information security controls according to their needs, using guidance and suggestions where relevant. Given the dynamic nature of information risk and security, the ISMS concept incorporates continuous feedback and improvement activities to respond to changes in the threats, vulnerabilities or impacts of incidents (ISO/IEC, 2018; ISO/IEC, 2011). The LEDA Group can continually improve the cybersecurity procedures through benchmarking and the application of a consistent internationally recognised standard. The Assess step in F-CSAET incorporates the guidance of ISO27032, ISO27005 and ISO27008; hence, the cyclical nature of the F-CSAET, the continuous feedback and continuous assessment of changes in the threats, vulnerabilities and impacts of incidents.

6.1.3 King IV

King IV is a corporate governance guideline in South Africa. Although King IV is not law, companies are required to comply with it. It is applied on the principle of apply and explain. King IV directs what is required regarding IT governance. Principle 12 says the governing body should govern technology and information in a way that supports the organisation in setting and achieving its strategic objectives. According to King IV, IT should form an integral part of the company's risk management. The board should ensure that information assets are managed effectively, and that a risk committee and audit committee should assist the Board in carrying out its IT responsibilities. King IV directs that the Board must approve policy and adopt standards and frameworks. The governance of IT must achieve CIA of information asset and achieve objectives (IoDSA,

2016). The LEDA Group can avoid the impact of cybersecurity breaches such as negative reputation, potential loss of revenue, and law suits by establishing and implementing a cybersecurity policy and complying with King IV.

6.1.4 COBIT 5

COBIT is a good-practice framework created by the international professional association ISACA for information technology management and IT governance. COBIT provides an implementable set of controls over information technology and organises them around a logical framework of IT-related processes and enablers (ISACA, 2012).

COBIT 5 provides guidance on the development of the information security principles and policies. According to COBIT 5, its guidance on information security aims at the following benefits: reduced complexity and increased cost-effectiveness owing to improved and easier integration of information security standards; good practices and/or sector-specific guidelines; increased user satisfaction with information security arrangements and outcomes; improved integration of information security in the enterprise; informed risk decisions and risk awareness; improved prevention, detection and recovery; reduced (impact of) information security incidents; enhanced support for innovation and competitiveness; improved management of costs related to the information security function; and better understanding of information security (ISACA, 2012).

LEDA Group can follow COBIT 5 in the implementation of the cybersecurity policy and procedures developed through King IV, ISO27001 and other ISO27000 series.

6.1.5 Protection Of Personal Information Act (POPIA)

POPIA is the law implementing the privacy rights enshrined in the Constitution of the Republic of South Africa. The law requires that all the policies, procedures, processes and practices in the organisations relating to personal information, are in fact protecting personal information. The LEDA Group cybersecurity policy should enable compliance with POPIA (Department of Justice, 2013).

6.1.6 Cybercrimes and Cybersecurity Bill in the Republic of South Africa

The Bill is in the process of becoming a law. The objectives of the Bill are: to create offences and impose penalties, which have a bearing on cybercrime; to criminalise the distribution of data messages which are harmful and to provide for interim protection orders; to further regulate jurisdiction in respect of cybercrimes; to further regulate the powers to investigate cybercrimes; to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrime; to provide for the establishment of a 24/7 Point of Contact; to further provide for the proof of certain facts by affidavit; to impose obligations on electronic communications service providers and financial institutions to assist in the investigation of cybercrimes and to report cybercrimes; to provide for the establishment of structures to promote cybersecurity and capacity building; to regulate the identification and declaration of critical information infrastructures and measures to protect critical information infrastructures; and to provide that the Executive may enter into agreements with foreign states to promote cybersecurity (Department of Justice, 2017).

The LEDA Group Board should take into consideration the aim of the Cybercrimes and Cybersecurity Bill when approving cybersecurity policies. This will benefit the company when the bill becomes law. The Group will be more mature in the application of the provisions of the new cybercrimes and cybersecurity law.

6.2 The input of CIT on the theoretical F-CSAET

The four-step theoretical framework in Figure 3.1 was presented to the Cybersecurity Interest Team (CIT) on 6 September 2018. The CIT proposed another step, Analysis, in Figure 6.2, be added as second step after Assess. The argument of the CIT was that the results of step one, Assess, should be analysed to identify potential root causes. The CSAET content should target the root causes. After consideration of the argument of CIT based on the principles of Abstraction and Benefit, the theoretical F-CSAET was refined to six steps. The steps respectively became Assess, Analysis, Create, Plan, Implement and Reinforce.

The CIT agreed with the researcher that step 1 and the added step 2 enabled the achievement of some of the secondary objectives identified in Chapter 1. Step 1 determines the current cybersecurity knowledge. Step 2 establishes potential drivers of

the current cybersecurity knowledge. The attitude and behaviour is found through ANOVA to be the direct result of current knowledge. The input of CIT and the results of analysis of the data collected from case study are further used to refine and add the other steps in the theoretical F-CSAET.

6.3 The steps and influence of data analysis

Chapter 5 analysed the data collected for each of the seven focus areas identified in Chapter 2. The relationship between knowledge, attitude and behaviour and how knowledge impacted on attitude and behaviour was inductively analysed. Each step of the theoretical framework within the context of the results of analysis of the data collected was discussed. The aim of data analysis was to move the theoretical F-CSAET to the real-world solution for implementing CSAET using the case study.

6.3.1 Assess

In order to implement relevant CSAET, cybersecurity risks, for which the vulnerability factor is human, should be identified and assessed in this phase (Da Veiga & Martins, 2017; Parsons et al., 2017). The current global cybersecurity threats, which succeed by exploiting human behaviour, should be identified and analysed. The analysis aims at understanding how such threats exploit human behaviour with the aim of breaching cybersecurity. Employee knowledge, attitude and behaviour towards cybersecurity should be assessed within this context in order to determine the gap that could lead to exploitable cybersecurity behaviour by the employees in their day-to day interface with their workplace computer (Öğütçü, et al., 2016).

In this research, HAIS-Q was utilised in the survey as the questionnaire. Proper approvals were obtained from the LEDA Group before the survey was conducted. The QuestionPro on-line facility was used as the medium of transmission for the questionnaire. The request to participate in the survey and the questionnaire were sent by email to employees with email addresses in the Group.

The relevance and validity of HAIS-Q was discussed in Chapter 5. Knowledge, attitude and behaviour were assessed for each of the three units of the seven focus areas in Chapter 5. The survey was voluntary and anonymous. Respondents were asked to respond on a Likert scale 1 to 5, from Strongly Disagree to Strongly Agree. The score 1

represented most unsecure cybersecurity behaviour, 3 represented undecided, 3.1 to 3.9 represented susceptibility area and 5 represented most secure cybersecurity behaviour. Reverse scoring was applied to all negative questions. The Assess step (Figure 6.2) is key in that it collects data, which provides substance for analysis.

6.3.2 Analyse

It is required that a gap between the benchmark and current cybersecurity knowledge be clearly defined and understood. Threats and vulnerabilities should be analysed for their sources and contrasted with the assessed employee cybersecurity knowledge, attitude and behaviour. The Analyse step determines to what extent or depth the CSAET programme should go. The Analysis step ensures that the CSAET programme gets the right response, the real cybersecurity KAB threats and vulnerabilities are loaded into the Create step. The areas where knowledge was found adequate are loaded into Reinforce step.

The survey results were analysed through the scoring criteria stated in the Assess step in Section 6.3.1. A mean of 1 represented most unsecure cybersecurity KAB; 3 represented undecided; 3.1 to 3.9 represented a susceptibility area; and 5 represented the most secure cybersecurity KAB. The ANOVA test in Table 5.2 shown that the results were consistent between knowledge, attitude and behaviour.

6.3.2.1 Password management

Using the same password, sharing passwords and using a strong password were each assessed for knowledge, attitude and behaviour. The results for password management attitude shown that the LEDA Group employees were likely to share passwords with colleagues. Although employees shown that they know passwords should not be shared, they seem to believe that if not sharing a password could stall the work progress, then it should be shared for the sake of achieving work objectives.

Results for password management in Section 5.3.1 shown that the KAB of the LEDA Group employees was at cybersecurity secure level, except for the sharing of passwords with colleagues. Sharing of passwords, Figure 5.1, by the LEDA Group employees score within the susceptible area. Sharing passwords as a unit for the focus area password management should go into the Create step in Figure 6.1.

Use of the same password and development of a strong password shown a mean in the secure cybersecurity KAB. These two aspects as units of password management go into the Reinforce step in Figure 6.2.

6.3.2.2 Email use

Clicking on links of an email from a known sender, clicking on links of an email from an unknown sender and opening an attachment from an unknown sender were each assessed for knowledge, attitude and behaviour. The analysis of the KAB results shown that the employees were susceptible to clicking on links of an email from a known sender, and opening an attachment from an unknown sender. Although employees shown good knowledge on opening attachments from unknown senders, the attitude and behaviour shown some level of vulnerabilities. The knowledge for clicking on links for an email from an unknown sender shown vulnerabilities even though attitude and behaviour shown secure levels.

Section 5.3.2 shown the mean of the email focus area within the susceptible level. Table 5.4 and Figure 5.2 demonstrate the actual level of cybersecurity knowledge on the email use area. Based on the knowledge levels, and the vulnerabilities and threats to the LEDA Group discussed in Chapter 2, email use goes to the Create step in Figure 6.1.

6.3.2.3 Internet use

Knowledge for downloading files from Internet and entering work information on line for the LEDA Group employees were found to be in the unsecure levels of cybersecurity. The behaviour regarding the downloading of files was in the unsecure levels of cybersecurity. The attitude for downloading files from Internet, knowledge and behaviour for accessing dubious websites, and attitude and behaviour for entering work information online were found to be susceptible to fall into unsecure behaviour by the employees. The cybersecurity secure knowledge level for accessing dubious websites did not translate into secure attitude and behaviour.

Analysing the implications of the number of areas where employees were found to be within unsecure and susceptible levels, are shown in Table 5.5 and Figure 5.3, against the threats such as virus and malware, which were discussed in Chapter 2. The Internet use focus area goes to the Create step in Figure 6.1.

6.3.2.4 Social media

The social media privacy settings were found in the susceptible level for both knowledge, attitude and behaviour. Both consideration of consequences before posting on social media and posting about work were found at secure level.

The social media privacy settings should be loaded into the Create step. Based on the overall analysis summarised in Table 5.6 and Figure 5.4, the social media privacy settings go to the Create step in Figure 6.1. The consideration of consequences before posting and posting about work go to the Reinforce step in Figure 6.2. The objective of Reinforce is to maintain and enhance the current adequate cybersecurity knowledge.

6.3.2.5 Mobile devices

Employees were found susceptible to sending sensitive information via Wi-Fi. The analysis of the survey results shown that for attitude towards sending sensitive information via Wi-Fi, employees were not quite sure about the riskiness of the action. Securing mobile devices and shoulder surfing were found to be in the secure level on both KAB.

Section 5.3.5 shown that the KAB for sending of sensitive information via public Wi-Fi requires attention. Table 5.7 and Figure 5.5 demonstrated the current knowledge and on that basis the sending of sensitive information via Wi-Fi knowledge unit goes to the Create in Figure 6.1. The KAB for securing mobile devices and shoulder surfing goes to the Reinforce step in Figure 6.2.

6.3.2.6 Information handling

The knowledge for inserting removable media found in public places into computers and laptops was found in the susceptible area. The summary, Section 5.3.6, of the analyses in Table 5.8 and Figure 5.6 shown the vulnerabilities. Based on these analyses and the desire to be on a secure level of cybersecurity knowledge, the KAB for inserting removable media found in public places into computers and laptops goes to the Create step in Figure 6.1. Disposing of sensitive print-outs and leaving sensitive material on the desk were found in the secure level and therefore go to the Reinforce step in Figure 6.2.

6.3.2.7 Incident reporting

The knowledge of ignoring poor behaviour by colleagues and reporting of incidents, the behaviour of ignoring poor behaviour by colleagues and the attitude of reporting incidents were found in the insecure level. The analysis is shown in Section 5.3.7, Table 5.9 and Figure 5.7. Based on the analysis of the results, the KAB for both ignorance of poor behaviour and reporting of incidents go to the Create step in Figure 6.1. Reporting suspicious behaviour was found in the secure level and therefore goes to the Reinforce step in Figure 6.2.

6.3.3 Create

The purpose of this step is to serve as a catchment area. The KAB areas requiring intervention are recorded into the Create area. The Create step is key in that at any given point it shows the areas of cybersecurity vulnerabilities. The contents in the Create area change as step 1 and 2 are performed and the new gap is identified.

The Create step is a reference point for cybersecurity content for the current CSAET needs. Figure 6.1 presents the gap of the cybersecurity knowledge for this case study. The current gap for the LEDA Group was determined through the analysis of data collected from employees. The implications of the ANOVA test performed were taken into account when determining the focus areas recorded into the Create step. In cases where either knowledge, attitude or behaviour was found to be at the unsecure level or in the susceptible area, the conservative position was taken on the strength of the ANOVA test that means are not significantly different. The overall analysis result for such units of the focus area was lowered to the unsecure or susceptible level. The aim was to leave nothing to chance as the impact of cybersecurity breaches are huge in the LEDA Group.

The Create box in Figure 6.1 is recorded with the units of focus areas identified earlier in this chapter.

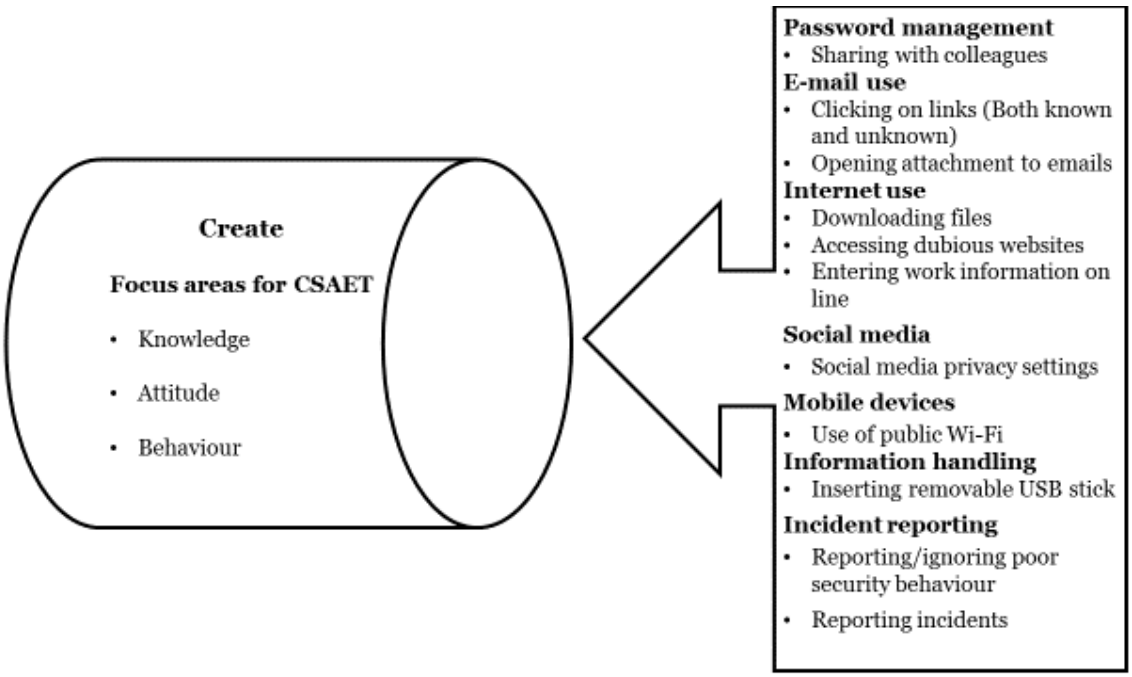

Figure 6.1: Create with the LEDA Group gap

6.2.4 Plan

A structured way of implementing CSAET is required to achieve the objectives of CSAET programme. The knowledge areas requiring CSAET from basic to reinforce level were deposited in the Create step. The other knowledge areas requiring maintenance and enhancement were deposited in the Reinforce step. A CSAET programme implementation strategy should be developed in this step. This involves setting measurable objectives, and resources required for the effectiveness of the programme. Programme delivery mode should be selected and the programme material should be developed. The content should be developed for both areas in the Create and Reinforce steps. The differentiating factor between the Create and Reinforce steps is the level of detail and attention required.

The approach for the Create step is from what to why, while for Reinforce it is why. At the Create step knowledge is built so that attitude and behaviour can change, while at Reinforce, knowledge, attitude and behaviour are maintained and enhanced. The development of material content and the choice of delivery mode should deliberately counter cognitive biases, such as the affect heuristic, anchoring, confirmation bias, availability heuristic, optimism bias, loss aversion and hyperbolic time discounting, as well as risk perception and the psychometric paradigm (Tsohou et. al., 2015).

Feedback mechanisms should be developed (e.g. preparation of e-learn assessment, and a survey for the general feed on the success of the programme) at this stage in order to enable evaluation of the efficiency and effectiveness of the programme. The Plan step, Figure 6.2, should enable answers to the following questions: Was the programme carried out as intended? Did the programme lead to the intended changes in cybersecurity awareness, attitude and behaviour? Why did the programme lead to changes or lack of such of awareness, attitude and behaviour? (Albrechtsen & Hovden, 2010).

The content for the LEDA Group CSAET was recorded in Table 6.1 and posted to either the Create or Reinforce step in Figure 6.2. Table 6.1 outlines the content for each focus area. The content was produced by the Analyse step. The mode of delivery may include animations and videos. Employees are given a timeframe to complete the e-learning programme.

Table 6.1: CSAET Content

Focus area	Minimum Content	
	Create	**Reinforce**
Password Management	Sharing of passwords • Risks of sharing passwords • Consequences of sharing passwords	Same passwords • Risks of using same password Strong passwords • Formulation of password • Bad passwords • Good passwords Create step knowledge
Email use	Clicking on email links • Risks of clicking on links both from known and unknown senders • Phishing • Recognition of phishing email • Social engineering • Recognition of social engineered email Opening email attachments • Risks of opening email attachments • Consequences of opening email attachments	Create step knowledge content moves to reinforce once employees adequate cybersecurity knowledge is achieved.
Internet use	Downloading files on internet • Risks and consequences of downloading files on the internet Accessing dubious websites • Risks and consequences of accessing dubious websites • Recognition of dubious websites Entering information on line • Risks and consequences of entering information on line	Create step knowledge content moves to reinforce once employees adequate cybersecurity knowledge is achieved.
Social media	Social Media privacy settings • Risks of unprotected social media settings • Social media privacy settings	Considering consequences of posting on social media • Considerations before posting on social media • Consequences of posting about work Create step knowledge
Mobile devices	Use of public Wi-Fi • Risks and consequences of sending information via public Wi-Fi	Securing mobile devices • Physical security Shoulder surfing • What is shoulder surfing • Risks of shoulder surfing Create step knowledge
Information handling	Removable media • Risks and consequences of inserting media found in public	Sensitive information • Disposing of sensitive print-outs • Leaving sensitive information Create step knowledge
Incident reporting	Poor behaviour by others • Ignoring poor behaviour by colleagues Reporting of incidents • Benefits of reporting incidents	Suspicious behaviour • Reporting suspicious behaviour Create step knowledge

6.2.5 Implement

To change attitude and behaviour, the Plan step must be implemented. The employees must interact with the CSAET programme. Combinations of resources identified in strategy and material development are put into process ultimately to effect change in behaviour regarding cybersecurity. The CSAET programme implementation methods should ensure psychological ownership by employees. A variety of training methods should be employed to immerse the participants in training during interaction sessions (Yoo et al., 2018). The programme must attempt to change behaviour in a manner that ultimately leads to a change in attitudes, that should also much more likely result in a long-term modification of behaviour (Thomson & Von Solms, 1998). A feedback mechanism is implemented to obtain feedback on the progress and success of the CSAET programme. The results of the feedback are analysed and the reinforcement programme is put in motion to ensure continuous learning.

At the end of the e-learning programme a certificate is issued to confirm competence of the employee on cybersecurity awareness and education. Employees not completing the e-learning task should face consequences in accordance with the policies.

6.2.6 Reinforce

The Reinforce step is the last to complete the F-CSAET, Figure 6.2. The step presents an opportunity to counter the truth that humans are forgetful creatures and, therefore, without immediate and continual reinforcement, a high percentage of the knowledge gained in the training phase will tend to evaporate quickly (Wozniak et al., 1995). There has to be a consistent continuous engagement with employees on all focus areas. This phase aims to achieve zero incidents emanating from human error or ignorance. Once the adequate level of cybersecurity knowledge is attained for areas in Figure 6.1, they are transferred to the Reinforce step where the cybersecurity knowledge is maintained and enhanced to change the attitude and behaviour.

This is an emphasis and re-emphasis step. The feedback from the implementation phase informs the content of reinforcement. The basis for this step is that behaviour cannot be changed by one training or session in one financial year. Methods such as knowledge sharing entrench awareness, ownership, and confidence in employees. The other positive outcome of knowledge sharing is that knowledge that comes from interactions

between collaborators, is less costly and more efficient (Safa & Von Solms, 2016). The CSAET programme is cyclical in nature and, therefore, the CSAET programme must be on a continuous improvement mode. As reinforcement is performed through continuous education and training, further assessment and analysis in the Assess and Analyse steps respectively, are conducted to fit into the Create step and ensure return for investment in CSAET. The continuous nature of CSAET programme requires adequate support from the top of the organisation and F-CSAET requires adoption by practitioners. The Reinforce step is fed from the Analyse step.

The Analyse step in the case study produced: use of the same password and use of a strong password as units for Reinforce for password management. Consideration of consequences and posting about work were identified for social media, and physical security of mobile devices and shoulder surfing were identified for mobile devices. In the other focus areas, disposal of sensitive print-outs, leaving sensitive material on the desk, and reporting of suspicious behaviour were identified for information handling and incident reporting respectively.

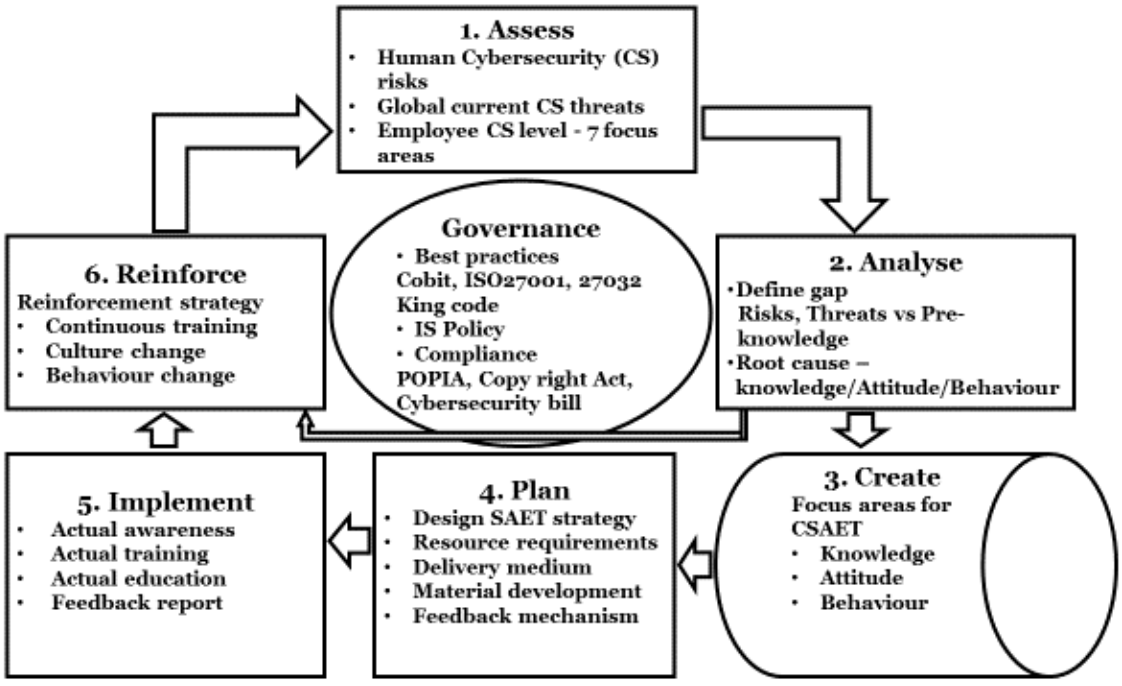

Figure 6.2: F-CSAET

6.4 F-CSAET validation

Ownership of the intervention is a prerequisite to effective implementation. Phase 3 of the NMU-DSFM in Chapter 4 requires that the practitioners validate the intervention before it is finalised, and diffused as required by phase 4 of NMU-DSFM. The second iteration with the Cybersecurity Interest Team took place on 11 October 2018. The Cyber Security Team made up of Head of Group IT operations, Deputy Chairman of Management IT Governance Committee, IT Audit Specialist and two Technicians, was established this purpose only. This became the final iteration as the participants reached the conclusion that the draft framework was an implementable intervention. The framework was evaluated at high level for the four principles of abstraction, originality, justification and benefit and the conclusion is shown in Figure 6.3. The conclusion confirmed that it is applicable to all classes of problems, will substantially contribute to the advancement of the body of knowledge, is valid, and can yield benefit immediately and in the future.

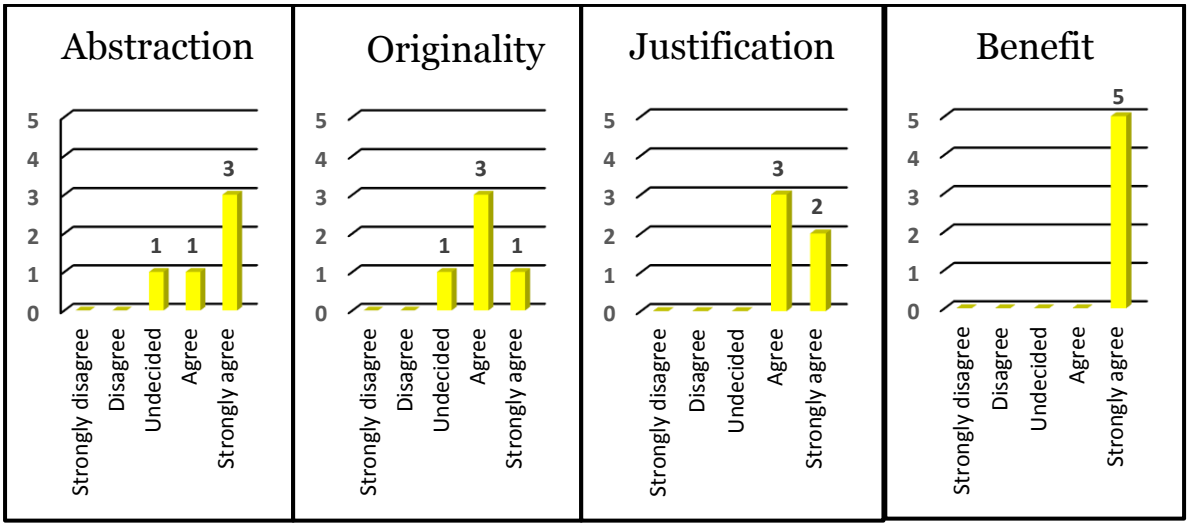

Figure 6.3: Principles of abstraction, originality, justification and benefit

6.5 Conclusion

The F-CSAET was developed in this chapter. Each step of the F-CSAET was identified and discussed. The F-CSAET was tested for applicability within the LEDA Group and in general through the Cybersecurity Interest Team. The LEDA Group can immediately implement CSAET programme applying the F-CSAET as the Create step has been filled with an inventory of the cybersecurity knowledge gap within the Group. The knowledge

gap was determined through survey analysis in Chapter 5. The worst results were found in email use (Figure 5.2) and Internet use (Figure 5.3) and the best results were found in information handling (Figure 5.6). The cyclical character of the F-CSAET makes it agile and enables it to remain in an improvement mode. Chapter 7 summarises the findings of this research; how the objectives were met; the contributions of the research; and identifies future research opportunities.

CHAPTER 7: CONCLUSION

Chapter 7 summarises the treatise. The Chapter summarises the findings of the research, discusses how the objectives set out in Chapter 1 were met, what contributions the treatise has made and the future research opportunities identified in through the research.

7.1 Summary of findings

It is clear that cybersecurity is a serious threat to the information asset in most organisations. Most organisation are largely dependent on information technology to conduct their businesses. This ever increasing dependence makes it absolute need for employees to have competent knowledge regarding cybersecurity. To ensure employees have competent cybersecurity knowledge, a structured way of implementing the programme delivering awareness, education and training is necessary. LEDA Group was used as the case study.

Chapter 2 discussed the structure and shape of the LEDA Group, the cyber risks, cybersecurity, cyber threats and vulnerabilities in the context of the case study. Furthermore, the role of employees, good cybersecurity behaviour and seven interface areas between employees and computer were identified. The seven focus areas formed the focal point for data collection as discussed in Chapter 5.

To achieve the training of competent cybersecurity knowledge to employees, the review of literature was required to determine the state-of-the-art or benchmark level. Chapter 3 reviewed literature to determine what the benchmark cybersecurity awareness, education and training should contain, what steps should be followed to address the real cybersecurity awareness, education and training needs. A theoretical F-CSAET was developed in Chapter 3 following extensive literature review. To localise the theoretical F-CSAET to the case study, collection of data from case study was required. The data collection required a research methodology and methods to be followed.

Chapter 4 identified and described the Nelson Mandela University Design Science Methodology Framework (NMU-DSFM) as the methodology to be followed. Human Aspects of Information Security-Questionnaire was identified and applied in Chapter 5 as a survey questionnaire. The questionnaire covered the seven focus area in terms of

knowledge, attitude and behaviour per area. On-line facility called QuestionPro was used to send the questionnaire to respondents and analyses of the responses. The cybersecurity knowledge gap was determined in Chapter 5 by analysing the survey results and contrasting them against the benchmark in Chapter 3.

Chapter 6 refined the theoretical F-CSAET developed in Chapter 3 applying the input of Cybersecurity Interest Team and the findings of the results analyses in Chapter 5. F-CSAET was developed. Although the LEDA Group was used as a case study, the F-CSAET is applicable to any organisation as the six steps applies in any environment and load step 3 with organisation specific cybersecurity knowledge gap.

7.2 Meeting the objectives

This study aimed to address real-world problem identified in LEDA Group. Chapter 1 stated the primary objective of this study as to develop framework to implement cybersecurity awareness, education and training within LEDA Group. In order to achieve the primary objectives, secondary objectives were developed and they were to determine the state-of-the-art regarding cybersecurity awareness, education and training; to assess the current knowledge of officials regarding cybersecurity; and to determine the gap between state-of-the-art and current knowledge.

To determine the state-of-the-art cybersecurity awareness, education and training, Chapter 3 reviewed literature to identify benchmark cybersecurity knowledge, attitude and behaviour over seven focus areas, namely, Password Management, Email use, Internet use, Social media, Mobile devices, Information handling and Incident reporting. The seven focus areas were identified in Chapter 2. The theoretical CSAET was developed based on literature.

Chapter 2 discussed the cyber threats and vulnerabilities of the case study, LEDA Group. Data from the employees of LEDA Group was collected and analysed in Chapter 5 in order to assess current knowledge and determine the gap between the current knowledge and the state-of-the-art cybersecurity knowledge.

Following the research methodology discussed in Chapter 4, refinement of theoretical F-CSAET developed in Chapter 3, results of analysis of data collected in Chapter 5, the

final F-CSAET was developed in Chapter 6. The F-CSAET was the primary objective of this research.

7.3 Summary of contributions

The research output was a framework. This framework, called F-CSAET, Figure 7.1 was extensively discussed in Chapter 6. The framework consists of six steps, Assess, Analyse, Quarantine, Plan, Implement and Reinforce. The six steps are supported by information security governance applying best practices. The six steps were discussed at length in Chapter 6. The adoption of this framework strengthens governance of information security in the organisation. Best practices were identified to ease reference as to what is required and how to implement the required regarding information security with specific focus on cybersecurity.

Although LEDA Group was used as case study, the F-CSAET is ready for implementation for any organisation without further adaptation as it complied with the research paradigm principles of abstraction, originality, justification and benefit. The implementation of the F-CSAET has the ability to turn human factor in cybersecurity the strongest link. The research identified sevens focus areas upon which the framework should be applied, namely, Password Management, Email use, Internet use, Social media, Mobile devices, Information handling and Incident reporting. These areas are key as they collectively form the interface of employees and the computer.

The F-CSAET pointed out that the success of cybersecurity awareness, education and training lied in the consistent and continuous application of the guidance provided by the F-CSAET. The implementation of F-CSAET aims at improving cybersecurity knowledge in order to change cybersecurity attitude and therefore human behaviour from bad to good cybersecurity behaviour.

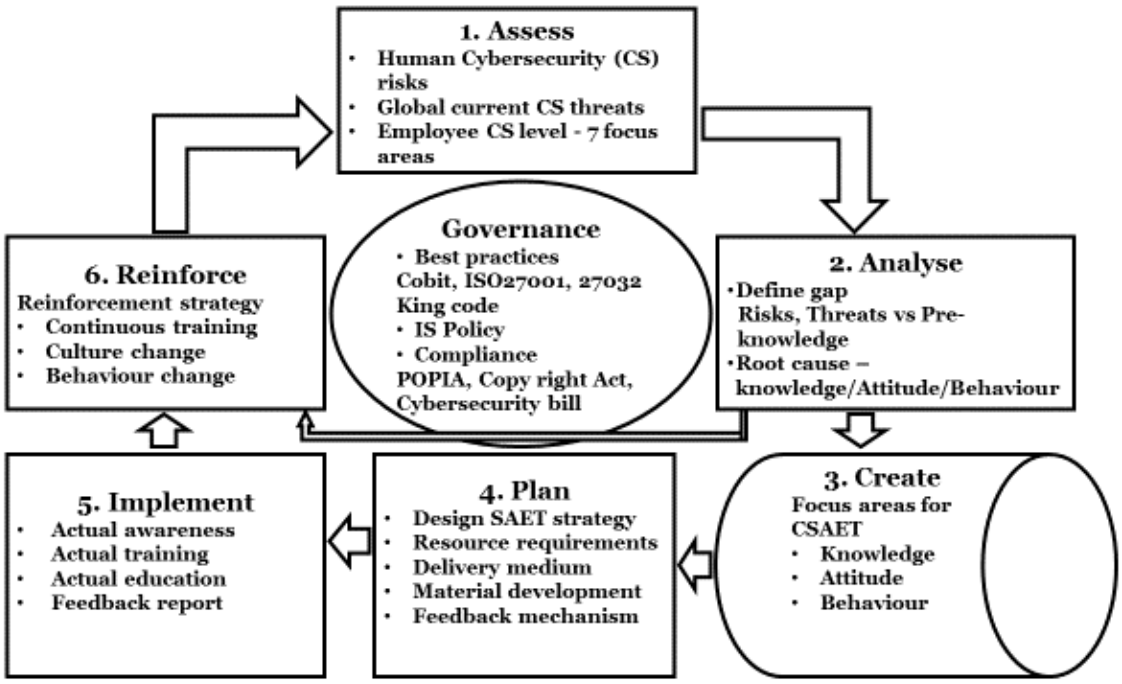

Figure 7.1: F-CSAET

7.4 Future research

As part of future research, it is suggested that the aspect of the medium of delivery of CSAET be investigated to provide opportunities for efficient and effective CSAET.

Another future research opportunity could be found in the research of cases where there is less cybersecurity knowledge, but good attitude and appropriate cybersecurity behaviour. In this research it was found that for certain focus areas, employees had low a mean for knowledge, but a high mean for attitude and behaviour.

The third future research opportunity could be found in an education technique to impact on the permanent retention of cybersecurity knowledge, attitude and behaviour.

7.5 Epilogue

This research developed the framework for the implementation of information security awareness, education and training with a specific focus on cybersecurity. Cybersecurity is a serious threat to many organisations although most organisations seem to be struggling in making employees their strongest link of prevention.

With the above in mind, the research developed F-CSAET which is applicable to any organisation. In so doing, this research contributed in the sense that the LEDA Group and other organisations should be able to implement appropriate and relevant CSAET by applying this F-CSAET.

REFERENCE LIST

Anti-Phishing Working Group 3rd Quarter 2017.
https://www.antiphishing.org

Arachchilage, N.A.G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in human behaviour*, 38, 304–312
https://doi.org/10.1016/j.chb.2014.05.046

Aurigemma, S., & Mattson, T. (2017). Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. *Computers and security*, 66, 218–234
https://doi.org/10.1016/j.cose.2017.02.006

Barton K., Lane, M., Tejay, G., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers and security*, 59, 9 – 25
https://doi.org/10.1016/j.cose.2016.02.007

Bryant, K., & Campbell, J. (2006). User Behaviours Associated with Password Security and Management. *Computers and security,* 14, 81-100
http://dx.doi.org/10.3127/ajis.v14i1.9

Butler, R. & Butler, M. (2015). The password practices applied by South African online consumers: Perception versus reality, *South African Journal of Information Management,* 17, 1-11
https://doi.org/10.4102/sajim.v17i1.638

Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computer and security*, 70, 72–94
https://doi.org/10.1016/j.cose.2017.05.002

Department of Justice, (2017). Cybercrimes and Cybersecurity Bill, Republic of South Africa, B6 – 2017
http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf

Department of Justice, (2013). Protection of Personal Information Act, Republic of South Africa, Act No. 4 - 2013
https://www.saica.co.za/technical/legalandgovernance/legislation/protectionofpersonalinformationact/tabid/3335/language/en-za/default.aspx

Drahošová, M., & Balco, P. (2017). The analysis of advantages and disadvantages of use of social media in European Union. *Procedia computer science*, 109, 1005–1009
https://doi.org/10.1016/j.procs.2017.05.446

Eberhagen, N., Giannakopoulos, G., Marinagi, C., Metalidou, E., Skourlas, C., & Trivellas, P. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia social and behavioural sciences*, 147, 424 – 428
https://doi.org/10.1016/j.sbspro.2014.07.133

Fimin, M. (2017). Are employees part of the ransomware problem? *Computer fraud and security,* 8, 15 – 20
https://doi.org/10.1016/S1361-3723(17)30072-6

Futcher, L., Safa, N.S., & Von Solms R. (2016). Human aspects of information security in organisations. Computer Fraud & Security, 2, 15-18
https://doi.org/10.1016/S1361-3723(16)30017-3

Gafni, R., Pavel, T., Margolin, R., & Weiss, B. (2017). Strong password? Not with your social network data. *Online Journal of Applied Knowledge Management* 5, 27-41
http://www.iiakm.org/ojakm/articles/2017/volume5_1/OJAKM_Volume5_1pp27-41.pdf

Gold, S. (2011). Understanding the hacker psyche. *Network security*, 12, 15 – 17
https://doi.org/10.1016/S1353-4858(11)70130-1

Gritzalis, D., Kastania, A., & Mylonas, A. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computer and security*, 34, 47 – 66
https://doi.org/10.1016/j.cose.2012.11.004

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Information Review*, 40, 265-281
https://www.researchgate.net/publication/299552211_Individual_processing_of_phishing_emails

Hampton, N., Baig, Z., & Zeadally, S. (2018). Ransomware behavioural analysis on windows platforms. *Information security and applications*, 40, 44-51
https://doi.org/10.1016/j.jisa.2018.02.008

Han, X., & Tan, Q. (2010) Dynamical behavior of computer virus on Internet. *Applied mathematics and computation*, 217, 2520-2526
https://doi.org/10.1016/j.amc.2010.07.064

Heartfield, R., & Loukas, G. (2017). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers and security*, 76, 101 – 127
https://doi.org/10.1016/j.cose.2018.02.020

Herrington, J., McKenney, S., Reeves, T. C., & Oliver, R. (2007). Design-based research and doctoral students: Guidelines for preparing a dissertation proposal. In C. Montgomerie, & J. Seale (Eds.), *Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications, 2007,* 4089-4097
https://ro.ecu.edu.au/ecuworks/1612/

Higgs, J.L., & Pinsker, R.E, Smith, T.J, Young, G.R (2016). The relationship between Board-level technology committees and reported security breaches. *Journal of Information Systems*, 30, 79–98

https://doi.org/10.2308/isys-51402

IoDSA, (2016). King IV – Report on corporate governance for South Africa, Johannesburg, South Africa
https://c.ymcdn.com/sites/iodsa.site-ym.com/resource/collection/684B68A7-B768-465C-8214-E3A007F15A5A/IoDSA_King_IV_Report_-_WebVersion.pdf

ISACA, (2016). Cybersecurity fundamentals glossary. Rolling Meadows, USA
https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf

ISACA, (2012). COBIT5 – Enabling processes. Rolling Meadows, USA
http://www.isaca.org/cobit/pages/cobit-5-enabling-processes-product-page.aspx

ISO/IEC, (2005). ISO/IEC 27001: 2005 Information technology - Security techniques – Specification for an information security management system. Geneva, Switzerland
https://www.iso.org/standard/42103.html

ISO/IEC, (2018). ISO/IEC 27005: 2018 Information technology - Security techniques – Specification for an information security risk management system. Geneva, Switzerland
https://www.iso.org/standard/75281.html

ISO/IEC, (2011). ISO/IEC 27008: 2011 Information technology - Security techniques – Guidelines for auditors on information security controls. Geneva, Switzerland
https://www.iso.org/standard/45244.html

Kearney, WD & Kruger, H.A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers and security*, 61, 46–58
https://doi.org/10.1016/j.cose.2016.05.006

Khan, G.F., Swar, B., & Lee, S.K. (2014). Social Media Risks and Benefits: A Public Sector Perspective. *Social science computer review*, 32, 606–627
https://doi.org/10.1177/0894439314524701

Kim H.Y. (2014). Analysis of variance (ANOVA) comparing means of more than two groups. *Restorative dentistry and endodontics*, 39, 74-77
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3916511/

Kleiner, C., & Disterer, G. (2015). Ensuring mobile device security and compliance at the workplace. *Procedia computer science*, 64, 274 – 281
https://doi.org/10.1016/j.procs.2015.08.490

Kruger, H., Drevin, L., & Steyn, T. (2007). E-mail Security Awareness: A Practical Assessment of Employee Behaviour. *Fifth World Conference on Information Security Education, eds. Futcher, L., Dodge, R. Boston: Springer*, 237, 33-40
https://link.springer.com/chapter/10.1007/978-0-387-73269-5_5

Li, T., Liu, L., Wang, J., Yasin, A., & Zowghi, D. (2018). Design and preliminary evaluation of a Cyber-Security Requirements Education Game. *Information and software technology*, 95, 179 - 200
https://doi.org/10.1016/j.infsof.2017.12.002

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers and security*, 34, 47-66
https://doi.org/10.1016/j.cose.2012.11.004

Oates, B. (2001). Cyber Crime. *How technology makes it easy and what to do about it. Information Systems security*, 9, 92 – 96
https://doi.org/10.1201/1086/43298.9.6.20010102/30989.8

Öğütçü, G., Testik, O.M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers and security*, 56, 83-9 3
https://doi.org/10.1016/j.cose.2015.10.002

Osterle, H., Becker, J., Frank, U., Hess, T., Karagiannis, D., Krcmar, H., Loos, P., Mertens, P., Oberweis, A., & Sinz, E.J. (2010).Memorandum on design-oriented information systems research. *European Journal of Information Systems,* 20, 7 -10
https://doi.org/10.1057/ejis.2010.55

Parsons, K., Butavicius, M., Jerram, C., McCormac, A., & Panttison, M. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and security*, 42, 165 – 176
https://doi.org/10.1016/j.cose.2013.12.003

Parsons, M., Butavicius, M., Calic, D., McCormac, A., Panttison, K., & Zwaans, T. (2017). Individual differences and Information Security Awareness. *Computer in human behaviour*, 69, 151 – 156
https://doi.org/10.1016/j.chb.2016.11.065

Pashler, H., Rohrer, D., Cepeda, N.J., & Carpenter, S.K. (2007). Enhancing learning and retarding forgetting: Choices and consequences*, Psychonomic Bulletin & Review,* 14, 187-193
http://www.pashler.com/Articles/Pashler.Rohrer.Cepeda.Carpenter_2007.pdf

Safa, N.S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in human behaviour*, 57. 442 - 451
https://doi.org/10.1016/j.chb.2015.12.037

Shay, R., Komanduri, S., Durity, L.A., Huh, P., Mazurek, L.M., Segreti S.M., Ur, B., Bauer, L., Christin, N., & Cranor, L.F. (2016). Designing Password Policies for Strength and Usability. *Management of computing and information systems*, 18, 1 – 34
https://www.archive.ece.cmu.edu/~lbauer/papers/2016/tissec2016-password-policies.pdf

Shen, C., Yu, T., Xu, H., Yang, G., & Guan, X. (2016). User practice in password security: An empirical study of real-life passwords in the wild. *Computers and security*, 61, 130 – 141

https://doi.org/10.1016/j.cose.2016.05.007

Silic, M., & Back, A. (2013). Factors Impacting Information Governance in the Mobile device dual-use context. *Records Management Journal*, 23, 73 - 89 https://www.emeraldinsight.com/doi/abs/10.1108/RMJ-11-2012-0033?journalCode=rmj

Siponen, M.T. (2000). A conceptual foundation for organizational Information Security awareness. *Information Management & Computer Security*, 8, 31-41 https://www.emeraldinsight.com/doi/abs/10.1108/09685220010371394

Social-Engineering Report by AGARI. 2016. https://www.agari.com

Thomson, M.E., & Von Solms, R. (1998). Information Security awareness. *Educating your users effectively*. *Information Management & Computer Security*, 6, 167-173 https://www.emeraldinsight.com/doi/abs/10.1108/09685229810227649

Wilson, M. & Hash, J. (2003) National Institute of Standards and Technology, Building an Information Technology Security Awareness and Training Program. Computer Security, 800, 50 https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf

World Internet Users and 2018 Population Stats: https://www.internetworldstats.com/stats.htm

Wozniak, P.A., Gorzelanczyk, E.J., & Murakowski, J.A. (1995). Two components of long-term memory. *Acta neurobiologiae experimentalis*, 55, 301-305 https://europepmc.org/abstract/med/8713361

Yang, X., Ren, J., & Zhu, Q. (2012). Modelling and analysis of the spread of computer virus. *Communications in nonlinear science and numerical simulation*, 17, 5117-5124 https://doi.org/10.1016/j.cnsns.2012.05.030

Yin, R. (2013). Validity and generalization in future case study evaluations. *Research article*, 19, 321-332 https://journals.sagepub.com/doi/abs/10.1177/1356389013497081

Yoo, C.W., Sanders, G.L., & Cerveny, R.P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision support systems*, 108, 107-118 https://doi.org/10.1016/j.dss.2018.02.009

Zhu, Q., Yang, X., & Ren, J. (2012). Modelling and analysis of the spread of computer virus. *Communications in nonlinear science and numerical simulation*, 17, 5117–5124 https://doi.org/10.1016/j.cnsns.2012.05.030