Monograph

A new dawn in Private Security: *The accreditation of Cybersecurity Training*

Executive Summary

Research Findings

Training Employers of cybersecurity officers averred that they do check whether the officers have training from an industry-recognised institution. The majority of the preferred cybersecurity certificates are not offered by South African-based institutions. In South Africa, few public universities offer cybersecurity qualifications.

There are also private institutions that offer cybersecurity training. Employers do not necessarily check whether an institution from where their employee was trained is accredited with any regulatory body in South Africa. If a candidate received a cybersecurity qualification from one of the highly preferred institutions, the prospective employer would not hesitate to appoint the candidate as a cybersecurity officer.

This brings another regulatory challenge as the legitimacy of these qualifications cannot be verified. The appropriateness of training received by cybersecurity specialists is arguably determined by industry standards and requirements. There is, however, no standardised reference material.

“It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it.” —

Stephane Nappo.

Table of Contents

CHAPTER 1

GENERAL ORIENTATION AND PROBLEM FORMULATION

1.1 Introduction

This chapter introduces the study's research topic and includes an overview of the project by explaining what it is about, why it is important, and who will benefit from it. The first section of the chapter outlines the study's intention and background. The discussion then moves to what prompted this research by elucidating the problem that it sought to understand and the new insights that were gained to better understand the dynamic nature of cybersecurity and its accreditation processes.

The study's aims, objectives, and the research questions are also outlined. Definitions of key concepts are provided, such as the internet, cybersecurity, cyberspace and accreditation. The chapter also presents an overview of the approaches the study employed to collect and analyse the data to draw conclusions that support the study's objectives. In addition, an outline of each chapter for the entire research study is presented.

1.2 Background of the study

The Fourth Industrial Revolution introduced electronics and information technology to society intending to automate production (Roberts, 2015). It is evident that this industrial revolution did not only bring about technological changes, but it introduced a concept of the internet which can be regarded as another world. Vrana (2012) maintains that the internet had become an environment that enables real-time dynamic interaction, facilitating global opportunities such as rapid communication, socialising, information and sharing, banking, the sale and purchase of goods and a vast array of business activities and information services.

The existence of the internet has made people’s lives easy all over the world. The statistics of the global digital population shows that in January 2021, there were 4.66 billion active internet users worldwide, which constituted 59.5 per cent of the world global population (Johnson, 2021). This means that the internet is utilised in many aspects. The increase in demand of the internet exposes its users to various criminal activities also known as cybercrimes (Vrana, 2012: 91 and Dubois & Jrejie, 2016: 178).

This study lays a foundation for the new dawn to private security. There is heavy reliance on digital platforms, computer systems and computerised processes of doing things and this creates a need to protect these aspects of people’s lives. Hence, many organisations worldwide have come up with strategies to safeguard their cyberspace. The new private security industry is called cybersecurity (Button, 2020).

As the world evolves, we continuously witness many changes occurring in a blink of an eye. As a key role player in the Safety and Security Sector South Africa, SASSETA must pay more attention to security services that emerge because of cyber-threats, namely cybersecurity services. Cybersecurity, by its very nature, is a broad concept that involves interesting components.

1.3 Problem statement

With the use of advanced technology at an all-time high, the value of security on the internet is even more crucial. According to a workforce study by the International Information System Security Certification Consortium (ISC), there are 3.4 million more skilled cybersecurity professionals needed globally right now (Button, 2020). But finding and retaining talent seems to be a difficult task as many people don't have the necessary skills and qualifications. The majority of the preferred cybersecurity certificates are not offered by South African-based institutions. In South Africa, few public universities offer cybersecurity qualifications. There are also private institutions that offer cybersecurity training.

Employers do not necessarily check whether an institution from where their employee was trained is accredited with any regulatory body in South Africa. If a candidate received a cybersecurity qualification from one of the highly preferred institutions, the prospective employer would not hesitate to appoint the candidate as a cybersecurity officer (Roberts, 2015). Hence, there is a need to investigate the accreditation of cybersecurity training providers.

1.4 The aim of the study

With the ever-evolving progress in digital technologies, societies have witnessed an increase in the number of individuals who are connected to the internet (Mungadze, 2019). The increasing number of cybercrime activities that occur in South Africa that need to be documented so that an enabling policy can be ratified to develop efficient cybersecurity measures to protect end-users. The aim of this study is to understand the investigate the accreditation of cybersecurity training providers.

The study thus critically analysed the effectiveness of legislations and their practical implementation to determine if the accreditation of cybersecurity training providers is efficient. Based on the findings, it is envisaged that this study will contribute to knowledge in the field of cybersecurity, prior to the study, very limited research was conducted to generate data regarding the accreditation of cybersecurity training providers.

1.5 Research objectives

This study seeks address the following objectives:

(i). Explore the accreditation of cybersecurity training providers.
(ii). Understand whether there is a regulator that is currently governing cybersecurity training providers.
(iii). Establish the role of South Africa's Internet Service Providers' Association in regulating and ensuring compliance of cybersecurity training providers.

1.6 Research questions

This study seeks to answer the following questions:

- What is the nature of accreditation services rendered to cybersecurity training providers?
- Is the accreditation of cybersecurity training providers effective?
- Which regulator is currently governing cybersecurity training providers?
- What is the role of South Africa's Internet Service Providers' Association in regulating and ensuring compliance of cybersecurity training providers?

1.7 Definition of key concepts

- **Internet:**

The internet is commonly known as “a worldwide set of computers using Transmission Control Protocol (TCP)/Internet Protocol (IP)” (Hitchcock & Page, 2016: 428). Furthermore, the internet is a global system of interconnected computer networks, that uses the IP suite to send and receive messages (Henning-Thurau, Gwinner, Walsh & Gremler, 2014). In this study the internet refers to the www where a system of interconnected computer systems operates, which requires the services of cybersecurity training providers.

- **Cyberspace:**

Cyberspace refers to the Internet or World Wide Web (*www*) and the culture that has emerged from it (Hitchcock & Page, 2006). Taylor & Spencer (2004) extend this definition by denoting cyberspace to a globally networked, multi-dimensional, artificial and virtual reality. It is sustained, accessed and generated by computers. In this study cyberspace refers to a virtual reality on the internet where cybersecurity services are required.

- **Online:**

This is the state of being when a person is linked to an Internet Service Provider (ISP), an American web portal and online service provider (AOL), and is e- or Earthlink connected (Sissing, 2013). Everything performed when linked to an ISP is considered to be online such as e-mails, browsing blogs, and when chatting or reading news bulletins online (Hitchcock & Page, 2006).

- **Accreditation:**

Accreditation is the act of giving credentials or authority to an educational institution when specific standards and quality of education being adhered to. Accreditation entails the evaluation of higher education academic programmes in accordance with the HEQC’s programme accreditation criteria, which stipulate the minimum requirements for programme input, process, output and impact, and review (Council of Higher Education, 2023).

- **Cybersecurity:**

The term "cybersecurity" has been the subject of academic and popular literature that has largely viewed the topic from a particular perspective. According to Craigen et al (2014) "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.

1.8 Research methodology

This research adopted a qualitative approach and the overall objective is to describe the social world, through comprehending, explaining, and discovering individuals experience and feelings in a great depth, from a human standpoint. Shuttleworth (2008) mentions that a qualitative research design has the advantage of being versatile and allowing for a wide variety of techniques for data collection and analysis.

1.9 Research design

Leedy (1997) describes a research design as a study plan that outlines the overall structure for data collection. Burns and Grove (2001) state that a clearly specified framework within which a study is implemented is referred to as its research design. This researcher used an exploratory study design which was embedded within the qualitative approach to provide a full analysis of the accreditation of cybersecurity training providers. Burns and Grove (2001:374) define exploratory research as “research that is performed to gain new insights, find new ideas, and increase knowledge of the topic under investigation”.

1.10 Sampling

In this study, purposive sampling technique was utilised to select the research participants. This method of sampling is appropriate when the researcher wishes to concentrate on a relatively small sample and in this case, the researcher selected a sample of ten (10) cybersecurity training providers. Sampling involves selecting a subset of the data population, to be used for participation in a study, based on a set of criteria (Polit & Beck, 2004; Uys & Basson, 1991).

1.11 Structure of research project

Chapter one, provides the background to the South African cybersecurity landscape. It also presents the purpose (or aim) of the study as well as its objectives and the research questions. It briefly refers to the study approach, provides insight into the cybersecurity phenomenon, and acquaints the reader with the research topic in general.

Chapter two, this chapter discuss the phenomenon of cybersecurity accreditation based on a review of scholarly literature and the South African legal framework that aims to address this crime. The discourse focuses on definitions of cybersecurity, the impact of cybersecurity on training providers, legislation that addresses cybersecurity in South Africa, and South African and global views of cybersecurity.

Chapter three, this chapter discusses the research methodology that was utilised in detail. Due to the nature of the study, the qualitative research approach was supported by an exploratory research design. This chapter also discusses the methods of data collection and analysis as well as the ethical considerations that were adhered to.

Chapter four, this chapter presents a summary of the results that emerged from the data analysis process. These results are in line with the research questions and objectives that directed the study. The discourse refers to findings from the literature and determines if the current study supported or refuted these results.

Chapter five, this chapter presents concluding remarks about the findings and offers some recommendations for future study.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter reviews literature on the accreditation of cybersecurity training programmes. The chapter further discusses the conceptual and theoretical frameworks underpinning this study.

2.2 Cybersecurity: A South African perspective

The dilemma that motivated this research is that individuals are becoming increasingly dependent on internet and computers, as digital technology progresses, however, millions of individuals are vulnerable to cybercrime because information can be easily and instantly transmitted in cyberspace. This emphasises the importance of implementing effective and efficient cybersecurity training providers.

South Africa has also suffered its largest data breach when approximately 60 million South Africans' personal data, including unique identity numbers of living citizens, deceased citizens and citizens living overseas were leaked (Venktess, 2017). Recently, in South Africa, a credit bureau called Experian has suffered a massive data breach that exposed information of 24 million individual South Africans and 800 000 businesses (eNCA, 2020).

The massive data leak included confidential information such as personal information, contact information and employment details. In another incident, the website of the local movie theatre Ster-Kinekor bookings leaked around seven million users' data. It was stated that there was a vulnerability in SterKinekor's back-end system of the old website. It allowed unauthorised people to access confidential data which included personal details, contact details, addresses and the passwords of all these users (Venktess, 2017).

Currently in South Africa, initiatives such as the Bill for Cybercrimes and Cyber Security have been established to deal with cyber issues (Department of Justice and Constitutional Development, 2017). This Bill primarily aims to promote cyber security to establish a support structure that promotes and builds capacity towards cyber security.

Furthermore, the Bill aims to establish a 24/7 Point of Contact to construct faults and enforce penalties which have a bearing on cybercrime within the country. The Bill aims to build a cyber security culture and promote cyber security for South African citizens. Therefore, South African cybersecurity should be provided with knowledge regarding cyber security so that they will be able to protect employees and customers against cyber threats.

The Bill also aims to enforce obligations for organisations to contribute to the investigation and reporting of cybercrimes within the country. As stated in the Bill, access to information about cyber security occurrences within the country is limited (Department of Justice and Constitutional Development, 2017). Information sharing concerning cyber security might be caused by the fact that some cyber incidents are not reported (PwC, 2016).

2.3 The New Private Security: Regulating Cybersecurity Services in South Africa

Organisations prefer to outsource cybersecurity services because they are more cost-effective than appointing in-house cybersecurity officers (Ding et al., 2005). One of the contributing factors for outsourcing cybersecurity services is the ongoing evolution of cyberattacks which requires them to provide refresher training to their cybersecurity officers every time, and the training is expensive (Ding et al., 2005; Pedley, Borges, Bollen, Shah, Donaldson, Furnell & Crozier, 2020).

Moreover, Ding et al., (2005) asserted that Managed Security Service Providers (MSSPs) have more experience, updated technology, better-trained expertise and serve diverse clients. The challenge that emerging MSSPs may face is that organisations that contract MSSPs will prefer those with more clients than emerging ones (Ding et al., 2005). These firms hold a view that having more clients also contribute to the improvement of service quality. A service provider that monitors more networks is more likely to correlate attacks, identify new attacking patterns and warn customers of events beyond their perimeters (Ding et al., 2005). Clients, therefore, indirectly contribute to the monopolisation of the industry. Button (2020) states that cybersecurity introduced new roles such as the role of moderators. He compared their activities in cyberspace to those of security guards in the physical world (Button, 2020).

He also maintained that they also share common traits such as low pay, high labour turnover, and having to deal with incidents that lead to a psychological toll on them (Button, 2020). Section 4(m) of the PSIR Act provides that the Authority must promote the protection and enforcement of the rights of security officers and other employees in the private security industry. By extension, CSSPs' rights must be protected by the PSIR Act. Button (2020) avers that some roles created by the newly emerged private security industry, such as testers or ethical hackers, have been occupied by the past criminal hackers because of their proven skills.

2.4 The impact of cybersecurity on critical infrastructure

According to Direnzo et al. (2015, p. 1), "computer networks control some of the most important critical infrastructures in the world". They refer to examples of critical infrastructures, namely power systems, water supply systems, air traffic control, building control systems, and transportation systems (Direnzo et al., 2015, p. 1).

In South Africa, when one refers to "critical infrastructure" they are referring to any infrastructure established in terms of section 16 of the Critical Infrastructure Protection Act 8 of 2019. Past research has shown that the increased interconnectivity of systems and reliance on technology by most critical infrastructures expose them to failures of computer systems and/or deliberate cyber-attacks (Direnzo et al., 2015; Pang, n.d.). Scholars argued that the most highly impacted critical infrastructures are the aviation and maritime sectors (Direnzo et al., 2015; Fox, 2016).

2.4.1 Cybersecurity awareness

Cyber security awareness is important and can be used to reduce cyber threats because many studies across the world use awareness to mitigate cyber threats (Grobler, Flowerday, Von Solms, & Venter, 2011a; Labuschagne & Eloff, 2012; Mbelli & Dwolatzky, 2016; Muhirwe, 2016; Parsons, Calic, Pattinson, Butavicius, McCormac, & Zwaans, 2017). Cyber security awareness helps in securing cyberspace and in providing support to promote an envisaged cyber security culture (Kortjan & Von Solms, 2014).

The purpose of awareness is to prepare internet users to have emergency plans in place against cyber-attacks (Rahim et al., 2015). Furthermore, cyber security awareness has been demonstrated to be an effective approach in reducing the threat of cyber-attacks associated with internet users (Muhirwe, 2016). Cyber security awareness is mainly designed in an attempt to prevent naive internet users from becoming targets of cyber-attacks (Grobler, Van Vuuren, & Zaaiman, 2011b).

This kind of awareness is vital to reduce cyber security threats that occur due to human-related vulnerabilities (Abawajy, 2014). Cyber security awareness is essential because it enables society to improve its cyber security practices while conducting activities within cyberspace (Alotaibi, Furnell, Stengel, & Papadaki, 2016). The establishment of cyber security awareness is the most preeminent method to fight cybercrimes (Alotaibi et al., 2016).

It is significant for people to have elementary knowledge about cyber security attacks and vulnerabilities (Tirumala, Sarrafzadeh, & Pang, 2019). When delivering cyber security awareness, the message must effectively reach people of all ages. It is also significant to ensure that knowledge about cyber security is transferred in such a way that the target audience receives acceptable 12 attention (Rahim et al., 2015).

2.4.2 Audience analysis for cyber security awareness

It is important to categorise users when conducting cyber security awareness to ensure that the relevant message is conveyed to the appropriate target audience. Numerous training methods are unsuccessful because they do not allow users to reflect and apply security concepts (Cone, Irvine, Thompson, & Nguyen, 2007). When conducting cyber security awareness, it is important to distinguish between multiple audiences which require different messages (De Bruijn & Janssen, 2017) because cyber criminals frequently target uninformed individuals with no or limited knowledge on how to recognise cyber-attacks.

In addition, when conducting cyber security awareness, it is important to analyse the target audience and consider the integration of multiple languages to avoid having skewed data due to language barriers (Grobler et al., 2011a), because in South Africa there are 11 official languages. Therefore, it is significant to provide tailored cyber security awareness with the integration of multiple languages.

2.4.3 Motivation for cyber security awareness

Technical measures independently are inadequate to solve critical IT security difficulties (Arachchilage & Love, 2014; Ramírez, 2017). Therefore, combining the usage of technical measures together with awareness might help to mitigate threats (Abawajy, 2014). Adelola et al. (2015) indicate that different materials can be developed to convey an appropriate message that is relevant to an audience’s needs and knowledge. (Alotaibi et al., 2016).

2.4.4 People are the weakest link

Several studies state that people are the weakest link within the cyber security chain (Abawajy, 2014; Anwar, He, Ash, Yuan, Li, & Xu, 2017; De Bruijn & Janssen, 2017). Professionals also agree that people are the weakest link regarding the protection of 13 information systems within organisations. People are frequently denoted as the first line of defence against several security threats (Parsons et al., 2017) because human error generally plays a role in cyber security breaches.

Yet, the best valuable technology-based security solutions not accompanied by awareness cannot deliver complete security which is required to protect organisational assets against prevalent threats (Abawajy, 2014). Cyber security breaches are widespread in organisations of all types and these breaches are frequently sanctioned by human errors (Anwar et al., 2017). These breaches can cause issues related to both financial and non-financial losses within a company and for its clients (Mbelli & Dwolatzky, 2016).

The literature revealed that cybersecurity concerns were solely the responsibility of internet service providers until the late 1990s when there were companies who established themselves as ISSPs (Allen, Gabbard, May, Hayes, & Sledge, 2003; Oppliger, 1997). Internet Service Providers (ISPs) and ISSPs are not the same despite other views to the contrary. It is our view that both ISPs and ISSPs are third parties that render different services to different markets for benefit. Saadat and Soltanifar (2014) state that ISPs generally refer to the people or companies that provide network and Information Technology (IT) support, wired and wireless telecommunications services required for internet access. Briefly, ISPs are internet access providers regulated by the Independent Communication Authority of South Africa (ICASA).

ISSPs refer to people or companies that protect internet users from cyber-related crimes using different types of managed security services (Ding, Yurcik & Yin, 2005). In short, their main aim is to provide security services and as the researcher observes, they are not regulated by any regulatory authority including ICASA because they are rendering security services in cyberspace.

This study excluded ISPs that exclusively provide ‘managed services. It is noteworthy to consider the argument advanced by Rowe et al. (2009) and Vrana (2012) that some ISPs are still offering different types of cybersecurity services to their clients. Therefore, ISPs that provide both services to their clients do form part of this study. Ding et al. (2005) assert that CSSPs render different security services to their clients. The following table formulated by Ding et al. (2005, p. 12) shows different types of cybersecurity services that are provided by MSSPs.

2.5 Fourth industrial revolution and cybersecurity

One would wonder why the background of the study did not discuss the Fourth Industrial Revolution (4IR), which was coined by Klaus Schwab in 2016. The motive behind this was that Xu, David and Kim (2018) argued that the Fourth Industrial Revolution is building on the Third Industrial Revolution, which was a digital revolution that has been occurring since the middle of the last century. They stressed that 4IR is characterised by a fusion of technologies that is blurring the lines between physical, digital and biological spheres (Xu et al., 2018). This means that cybersecurity services did not emanate from the 4IR. The recent industrial revolution witnessed the advancement of those security services which commenced in the Third Industrial Revolution. It is for this reason that the literature review focused on the Third Industrial Revolution in understanding the phenomena.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

This chapter discusses the DSRM research methodology which was used for this study to answer the research questions.

3.2 Research design process

3.2.1 Research philosophy

Research paradigms describe the fundamental philosophical understanding of clusters of people about the world in which they reside and the research studies they conduct (Oates, 2006). The research paradigms can be considered as basic sets of beliefs that are responsible to guide action (Creswell, 2014; Guba, 1990). A paradigm in information systems and information technology is for providing guidance in research within this field and in the process of constructing and implementing systems. A worldview can be described as a common philosophical orientation about the world and the nature of research that a researcher brings to a study (Creswell, 2014).

The research philosophy is mainly concerned with rigorously forming, regulating and enhancing the methods which are liable for creating knowledge (Partington, 2002). The research philosophy displays the perception of a researcher and the starting point for the research, such as the nature of knowledge as observed by the researcher (Bryman, 2016; Buthelezi, 2017).

Research philosophies are not in competition with one another. However, the philosophies vary due to the desired objectives of a study. The selection of research philosophies is based on the suitability and probability of achieving desired objectives (Buthelezi, 2017). The selection of

research methods and strategies are dependent on the research philosophical standpoints (Saunders, Lewis, & Thornhill, 2007). Therefore, based on the philosophical grounding, a discussion regarding the types of research perspectives or paradigms applicable to information systems and information technology and related research (positivist, interpretive, critical research and design science research) follows below.

3.2.2 Paradigm research

Paradigms are discussed in terms of characteristics and the suitable paradigms are selected. The possible philosophical assumptions for this study will be adopted from the matrix of Adebesin (2011) as shown in Table 3-1. This table provides a list of important characteristics to be considered in the implementation of the subsequent research paradigms. The research paradigm used for this study is represented by the last column titled “This study” in which N stands for No, while Y stands for Yes.

Table 3-1: Philosophical assumptions of the four research paradigms (Adebesin, 2011; Terre-Blanche et al., 2006)

Research Paradigm	Philosophical Assumptions				
	Ontology	**Epistemology**	**Methodology**	**Axiology**	**This study**
Positivist	Single, stable reality Law-like	Objective Detached observer	Experimental Quantitative Hypothesis testing	Truth (objective) Prediction	N
Interpretive	Multiple realities Socially constructed	Empathetic Observer subjectivity	Interactional Interpretation Qualitative	Contextual understanding	Y
Critical/ Constructionist	Socially constructed reality Discourse Power	Suspicious Political Observer constructing Version	Deconstruction Textual analysis Discourse analysis	Inquiry is value bound Contextual understanding	N
Pragmatism	Practically	Objective or subjective	Mixed methods Quantitative Quantitative Design-based research Action research	Value-free/ biased	Y

As shown in Table 3-1, only applicable research paradigms will be discussed:

- **Interpretive research paradigm:**

In this paradigm, access to reality is shown through social constructs such as language, consciousness, shared meaning and instruments. The focus is on the difficulty of creating human sense (Myers, 2013). An interpretivist believes that reality is disproportionately complicated to regulate every variable in it.

The role of the researcher in an interpretative research paradigm is to discover a systematic method of understanding circumstances within its natural setting (Buthelezi, 2017). Based on the interpretivist perspective, researchers attempt to understand in what way participants distinguish between situations (Buthelezi, 2017; Deetz, 1996).

- **Pragmatic research paradigm:**

In this paradigm, gaining knowledge is regarded as a continuum (Goles & Hirschheim, 2000). It accommodates studies that do not neatly fit the requirements of positivism or interpretivism (Alghamdi, 2013; Kortjan, 2013). The focus is on choosing methods that are most applicable, appropriate and relevant to the research. In addition, the research is determined by interest, value and relevance (Meyer, 2017; Van Zyl, 2015).

If the research is not clearly determined as to whether to adopt an interpretivist or positivist paradigm, then pragmatism is a suitable choice (Buthelezi, 2017; Saunders et al., 2007). March and Smith (1995) and Hevner, March and Park (2004) identify pragmatism as a paradigm relevant to DSRM. This study used interpretative and pragmatic paradigms to explain the fundamental philosophy depicted in Table 3-1. The pragmatic paradigm is applied to the DSRM and the interpretative paradigm is used in the design, demonstration and evaluation of the artefacts.

3.2.3 Research design

The research approach mainly gives details regarding the connection between theory and reality (Bryman & Bell, 2015; Buthelezi, 2017). There are two types of research approaches which can be adopted by a study, namely the deductive and inductive approach as explained in Table 3-2.

Table 3-2: Deductive and inductive research approach characteristics (Bryman & Bell, 2015; Buthelezi, 2017; Creswell, 2014; Gcaza, 2017; Hesse-Biber & Leavy, 2010; Robson, 2002; Saunders et al., 2007; Silverman, 2013)

Characteristics of research design	
Deductive	**Inductive**
The research is initiated by developing a research hypothesis.	The research is initiated by observing and searching for patterns in the data.
Examines a theory against data.	Produces a theory from data.
This approach is suitable for the positivist philosophy.	This approach is more appropriate for interpretive philosophy.
This approach uses scientific principles to confirm data validity and to enable the overview of the research findings.	This approach is recognised as a potential method to decrease possible researcher bias during the process of data collection.
The approach starts from general to particular. In addition, it uses a top-down approach.	The approach starts from particular to general. Therefore, it uses a bottom-up approach.
Quantitative in nature.	Uses a qualitative approach.
Works with variables.	Research content is investigated.

The inductive research approach is the best approach to utilise if there is minimal research that exists towards the research topic (Buthelezi, 2017; Saunders et al., 2007). This approach is much more flexible because it enables the focus of the research to change during the process of the research study, and that provides the researcher with more understanding. In conclusion, the inductive research approach was used in this study based on the discussion provided in Table 3-2. In addition, the inductive approach was used while demonstrating and evaluating the accreditation process status and process of cybersecurity training providers through expert interviews.

3.2.4 Research approach

A research methodology impacts a series of actions to be undertaken by the researcher throughout the course of collecting data to be used for a study (Myers & Avison, 2002; Ouma, 2013) in order to answer a set of research questions (Ouma, 2013). A variety of research strategies are derived from qualitative, quantitative and mixed methods research (Creswell, 2014; Ouma, 2013). Qualitative research regularly focuses on words from research participants to develop meanings. In addition, qualitative research pertains to describing small groups.

This methodology attempts to find knowledge about a certain occurrence through the interpretation and ability to understand the perceptions of the research participants (Meriam, 1998; Ouma, 2013). Contrarily, a quantitative methodology focuses on the process of testing research hypotheses to test existing theories (Ouma, 2013; Welman & Kruger, 2001). The mixed methods methodology complements both the qualitative and quantitative methodologies to conduct a particular research study. A combination of the two methodologies is used only during the collection and analysis of data (Creswell, Clack, & Vicki, 2007; Ouma, 2013).

3.5 Research strategy

A research strategy is a process of planning by the researcher and this plan determines how the study will be conducted (Creswell, 2014). The research strategy helps with determining the most suitable method to address the research aims and objectives, and also with monitoring the method of answering the research questions (Buthelezi, 2017; Ezzy, 2013). In addition, research strategies are utilised to answer the research problem and to meet the research objectives. In information systems research, there are various research strategies that are available for application.

Those research strategies include the following: experiments, surveys, case studies, archival studies, ethnography, grounded theory, interviews and systematic literature reviews (Buthelezi, 2017; Hofstee, 2006; Leary, 2016; Swanborn, 2010). However, the selection of the research strategy will be led by the research question(s), research problem and research objectives set by the researcher.

Furthermore, the research strategy will be led by the range of existing knowledge, the availability of timeand other resources at hand. In addition, the selection of the strategy will be affected by the philosophical underpinnings (Gcaza, 2017; Saunders et al., 2007). In conclusion, the DSRM is suitable to answer the research questions related to human problems by establishing artefacts. The output of the study was demonstrated and evaluated through interviewing expert reviewers.

3.5.1 Data collection techniques

In research, a variety of instruments can be used to collect the required data to answer certain research questions. Table 3-3 discusses some of the frequently used research instruments that researchers can use for data collection. The data collection methods used for this study are represented by the last column titled “This study” in which N stands for No, while Y stands for Yes.

Table 3-3: Data collection techniques (Creswell, 2014; Kumar, 2011)

Data collection/ types	Advantage	Disadvantage	This study
Questionnaires (Quantitative)	This method is costeffective and provides greater anonymity.	In this method, responses from participants cannot be supplemented with other information. In addition, this method is a self-selecting bias.	N
Interviews (Qualitative)	Researchers have control over the questions to ask participants.	Researchers might receive biased response from participants.	Y
Systematic literature reviews (Primary and Secondary) Documents (Qualitative)	These allow the researcher to understand the perception of participants better and the information can be accessed at any given time.	Researchers should search hard to find information which is time consuming.	Y
Observation (Qualitative)	Researchers have the ability to record available information.	The researchers can be regarded as intrusions.	N

For this study, a systematic literature review was conducted to discover research gaps and to answer research questions.

3.5.2 Systematic literature review

The systematic literature review was conducted and represented in Chapter 2. This systematic literature study provided an overview concerning South African research studies addressing cybersecurity. In addition, it provided a discussion about cyber security awareness components.

The systematic literature review covered the following topics:

- EXPLAINING THE COMPONENTS OF THE CYBER SECURITY AWARENESS FRAMEWORK
- THE INTERMEDIATE FRAMEWORK OF CYBER SECURITY ACCREDITATION

3.5.3 Expert review and Sampling

Purposive sampling was used to select 10 cybersecurity training experts/ personnel to refine and validate the components of cybersecurity accreditation as extracted from the literature review. These experts were selected based on the following experiences:

- Cyber security awareness
- Cyber security practice
- Science and technology
- Accreditation

This sampling method allows the researcher to select participants who will provide detailed information (Babbie, 2020; Ouma, 2013; Sami, 2016; Welman & Kruger, 2001). These selected experts were granted access to information about the study, These expert reviewers were selected based on their experience in the South African research domain and other relevant criteria. In addition, the data collected from interviews were utilised to ensure the trustworthiness of the study.

3.5.4 Data analysis

Data analysis is the procedure of interpreting and summarising collected data to discover patterns, relationships and trends within the research area. In qualitative research, data analysis proceeds from data collection to creation of reports based on findings (Creswell, 2014). In addition, to analyse data qualitatively, the researcher must first collect, organise and prepare data. Then the researcher must observe the data collected. Data analysis methods include the following:

- Thematic analysis:

Thematic analysis is correlated with interviews in terms of analysing the results (Jugder, 2016). This data analysis technique helps with the process of analysing data to provide meaningful information which is understandable.

- Hermeneutic analysis:

Hermeneutic analysis is related to understanding written information as well as understanding the connection between individuals, organisations and information technology (Myers, 2013). Hermeneutics assists with the process of interpretation because it is concerned with theories related to the proper manner of interpreting text (Schmidt, 2016). In addition, this data analysis technique can be applied when conducting interpretive research.

- Descriptive statistics:

Descriptive statistics is related to describing, comparing and summarising information numerically (Saunders et al., 2007). Descriptive statistics can be applied by analysing data using tables, charts and graphs.

- Content analysis:

Content analysis can be defined as a method of conducting a comprehensive and systematic analysis on data in order to identify patterns (Leedy & Ormrod, 2001). This data analysis technique helps with studying and analysing data for similarities or differences to understand the content of data analysed.

In this study, both thematic analysis and hermeneutic data analysis was applied. Thematic analysis was applied for analysing data obtained from expert interviews. Thematic analysis is suitable because it offers a purely qualitative, comprehensive and refinement justification of data (Braun & Clarke, 2006).

The systematic literature review was interpreted and analysed using the hermeneutic data analysis because hermeneutic process recommends constant re-interpretation of data to gain a more comprehensive understanding of relevant publications (Boell & Cecez-Kecmanovic, 2010). This process includes reading, analysing, reflective writing and interpretation in a rigorous manner (Laverty, 2003). The hermeneutic data analysis method was also used for interpreting and analysing feedback from expert reviewers.

In hermeneutic data analysis, it is important for information (in the form of text) acquired from interviews and a systematic literature review to be understood because “the more the process is reiterated (the fusion of horizons achieved), the more comprehensible the text becomes and the ‘greater’ the interpreter's understanding of the text becomes” (Introna, 2011, p. 242).

3.6 Design Science Research Methodology (DSRM)

The objective of this study is to ascertain the accreditation and certification of cybersecurity courses. Therefore, the DSRM was applied in this study to address the main aim of the research and to provide a response to the formulated research questions. DSRM is a research approach in which research questions that are relevant to human problems through the establishment of innovative artefacts are answered, thus contributing new knowledge to the body of scientific knowledge. The designed artefacts are both useful and important in understanding the identified problem (Hevner & Chatterjee, 2010).

Furthermore, DSRM mainly focuses on creating or advancing an artefact to improve its effectiveness and also validating the artefact by measuring its utility. This section provides a discussion concerning the importance of DSRM and its types of artefacts provided by March and Smith (1995), guidelines of DSRM by Hevner et al. (2004) and the DSRM process of Peffers et al. (2007).

March and Smith (1995) have conducted a study to compare design science (prescriptive research) and natural science (descriptive research). According to March and Smith (1995), DSRM is an activity that uses knowledge with the aim of improving whatever that it is applied to.

- **Construct:**

Is the conceptual vocabulary for describing a problem or solution, and it creates specifications for problems and solutions. A construct must show comprehensiveness, elegance, ease of use and the ability to be understood.

- **Model:**

Is a set of statements that can be utilised for expressing the relationships between constructs. Model is a representation of the identified problems and future solutions. Model can also be referred to as a concept and illustration of a problem or solution which includes frameworks and guidelines. In DSRM, models are concentrated on their usefulness or effectiveness. A model must demonstrate dependability to real-life phenomena, accuracy, robustness and reliability.

- **Method:**

Is a set of stages that provides guidelines on performing tasks which illustrate a planned series of actions for accomplishing a certain goal. Method can also be defined as a procedure that specifies how to solve identified problems and developing future solutions. In DSRM, a method that intends to effectively solve an existing problem is regarded as valuable. The method must be in operation.

- **Instantiation:**

Is the operationalisation of a construct, model or method. Instantiations illustrate the competence, practicability and usefulness of the constructs, models or methods for the environment and its users. The Csa4Cybersecuritys {RSA} framework is an example of this artefact.

- **Better theories:**

Are the artefact construction as corresponding to experimental natural science. DSRM can contribute by formulating better theories or developing new ones. Developing or evaluating an artefact assists with improving an understanding of the correlation between elements, which could possibly result in the process of developing a new design theory for an artefact.

3.7 Guidelines for carrying out Design Science Research Methodology

This sub-section discusses each guideline in detail for carrying out DSRM as provided by Hevner et al. (2004). It also illustrates how each guideline was applied in this study.

Guideline 1: Design as an artefact

This guideline refers to the solution in the form of a determined IT artefact which is created to address problems within an organisation (Hevner et al., 2004).

Guideline 2: Problem relevance

This guideline worries about the relevance of the research for the information systems community. According to Hevner et al. (2004), the research must address encountered problems and opportunities that are afforded through the collaboration of people, organisations and IT.

Guideline 3: Design evaluation

This guideline relates to the gathering and analysis of related data to validate the usefulness, quality and efficiency of the designed artefact (Hevner et al., 2004).

Guideline 4: Research contribution

In this guideline, the developed artefact must resolve an unsolved problem or a known problem in a more operational or well-organised manner. Furthermore, the developed artefact must contribute to the existing body of knowledge (Hevner et al., 2004).

Guideline 5: Research rigour

This guideline ensures that the research follows the rigorous process to create and evaluate the designed artefact (Niehaves, 2007)

Guideline 6: Design as a research process

This guideline emphasises the perception of a well-designed artefact. The search of an effective artefact requires iteration to reach anticipated results (Hevner et al., 2004; Niehaves, 2007).

Guideline 7: Communication of the research

In this guideline, Hevner et al. (2004) recommend that findings of the design science research must be well-communicated to a variety of audiences including researchers, technologists, managerial personnel and others. In conclusion, a table below is provided to indicate how the research study applied the guidelines of DSRM.

3.8 Research ethics

A discussion of ethical issues is an unavoidable section to which any researcher should attend. In general, this research process brings tension to the connectivity between the objectives of generalising the research outcomes on behalf of the involved individuals, and the right to preserve the privacy and confidentiality of the participants in the study. They must have a right to anonymity. The participants in a research study must participate voluntary and sign the consent agreement. This process ensures that participants of the study and any other people are protected from any form of harm during participation.

CHAPTER 4

INTERPRETATION AND PRESENTATION OF FINDINGS

4.1 Research findings

This part presents the analysis and interpretation of the data collected in this study. In doing so, it provides answers to the research questions detailed in the research methodology.

4.2 The Existence of cybersecurity training providers

The common denominator for such existence is the obvious existence of cyberspace and criminal activities created by the ‘lack of guardianship’ within that space. There was an excellent opportunity to make money while protecting and safeguarding that space for others. It may be argued that during the formation of these training providers, the objective was to be proactive or reactive towards cybercrime. The reality is that their formation was associated with profit maximisation and ‘lack of guardianship’ within the country’s cyberspace.

4.3 The impact of cybercrime in South Africa

The weaknesses of State Information Technology Agency (SITA) networks allowed criminals to exploit the government Information Technology (IT) systems. The government witnessed an evolution of financial fraud within its institutions, which necessitated different measures to be put in place to prevent such criminal acts. It was gathered that the government was losing a lot of money because of the criminal syndicates who were creating ghost employees and contractors and stealing data to sell it to outsiders. After realising that the type of financial fraud which they were exposed to was not because of a physical security breach but a cybersecurity breach, the government decided to call upon experts in the field of cybersecurity to protect their cyberspace against various forms of cybercrime. Some of these experts started to form companies to provide cybersecurity services.

The concern of cybercrime was both in the public and private sectors. As aforementioned, the reasons for their existence may be proactive or reactive. Some companies stated that when they started offering cybersecurity services, their focus was more on the reactive approach to cyber incidents than being preventative. As time went by, they began to promote a proactive approach to cybercrime. They invited the public and private sectors to get on board in limiting opportunities for cybercrime to take place. The private sector had more opportunities for cybersecurity training providers to source clients than the public sector. This is one of the reasons why there are many companies offering cybersecurity services in the private sector than in the public sector.

4.4 Internet service providers ISPs migrating to cybersecurity

There are ISPs whose primary objective is to provide internet access to the people and organisations who end up putting cybersecurity services or internet security services as a value-added service to their clients. Other ISPs completely migrated to cybersecurity. The reason behind is none other than profit maximisation and taking advantage of ‘the lack of guardianship’ within cyberspace.

It was stressed that clients would appreciate the work of ISPs in providing them with access to the internet. After accessing the internet, the client would seek advice from the ISP on how to secure their network. Due to the ISP’s drive for profit maximisation, they never say they do not provide cybersecurity services. They sometimes inform their clients that they also provide cybersecurity services, which is incorrect. If the client gives them the job, they would subcontract this service to a company with such expertise. These companies would advertise for cybersecurity services and subcontract once contracted. This is how some ISPs are contracted to ‘offer’ cybersecurity services. There are a lot of ISPs in the country that provide cybersecurity services, however, one needs to take into consideration the fact that their primary function is not to protect but it is to provide access to the internet.

4.5 The Motive behind cyberattacks

The motive behind cybercrime varies from one individual and/or group to another. Most cybercrimes are economically and politically motivated. Politically motivated cybercrimes are not on the high end in South Africa as compared to First World countries.

Some people are just mischievous in testing their skills by hacking computers. Dubios and Jreije (2006) observed that some internet-related crimes were invented by unscrupulous individuals with the intent to steal, trespass, cause vandalism, “prove themselves to be elite hackers”, or just for thrill and challenge. These characters do this just for the fun of it without expecting anything in return.

Other individuals commit cybercrimes because of bitterness, desperation and anger. The anger may stem from being dismissed from an organisation. They may commit cybercrimes with the aid of a cybercriminal. An employee may also steal data from the organisation to defraud it. Sometimes an employee may steal data to sell it.

4.5.1 The Requirements for cybersecurity specialist(s) within cybersecurity

The requirements for specialising in specific cybersecurity roles are not determined by any law. A client determines who qualifies for a specific cybersecurity role. Employers use their experience and expertise in the field to develop job specifications. As aforementioned, there are different occupations within cybersecurity and each of them requires unique skills and/or qualifications.

For instance, requirements for an ethical hacker or penetration tester differ from those of a forensic investigator or cybersecurity consultant, even though these are referred to as cybersecurity officers or specialists. The name, ”cybersecurity officer” and/or “specialist” is very broad as it refers to any individual who renders security services in cyberspace, whether employed or self-employed. It is, therefore, impossible to uncover each requirement for cybersecurity roles.

An employer of a cybersecurity officer determines the minimum requirements for any cybersecurity position. Some companies appoint an officer with a matric certificate and train them to be a cybersecurity officer. Others only appoint those with a post-matric certificate in different fields of cybersecurity. Usually, cybersecurity companies require internationally recognised qualifications. There are cybersecurity roles that require specialists with a technical background, such as those with qualifications in IT, computer science, cybersecurity, or any related course.

There is also an emphasis on a strong technical experience. Some companies require specialists to develop policies, which does not require any technical experience. A person with forensic investigation or any criminology degree may be useful if a company requires a specialist that can adduce evidence in a court of law. It is important to note that there are no employment restrictions within cybersecurity as clients can hire a person from anywhere in the world. This is because there are no legislative requirements. This is different from the physical security environment, where it is categorically stated that only South Africans or permanent residents can render security services.

Thus, in the cybersecurity space, geographical restrictions are not applicable. In some instances, companies would do background checks and that is possible with South African or permanent residents. The recruitment and/or contracting from other countries presents a regulatory challenge. For instance, a person who is not vetted may provide a cybersecurity service in South Africa, thus compromising state security, especially where there is sensitive information involved.

4.5.2 The accreditation of cybersecurity training providers

Training Employers of cybersecurity officers averred that they do check whether the officers have training from an industry-recognised institution. The majority of the preferred cybersecurity certificates are not offered by South African-based institutions. In South Africa, few public universities offer cybersecurity qualifications. There are also private institutions that offer cybersecurity training. Employers do not necessarily check whether an institution from where their employee was trained is accredited with any regulatory body in South Africa.

If a candidate received a cybersecurity qualification from one of the highly preferred institutions, the prospective employer would not hesitate to appoint the candidate as a cybersecurity officer. It was noted that those who train at CISM are guaranteed of being hired by an audit firm and those who train at OSCP are guaranteed of being hired as pen testers. The following are preferred cybersecurity qualifications and institutions, which guarantee very high chances of cybersecurity employment in South Africa.

Qualifications Institutions
1. Certified Information Systems Security Professional International Information System Security Certification Consortium – (ISC)^2
2. Certificate in Cyber Security University of Johannesburg (Centre for CyberSecurity).
3. CompTIA Security+ Computing Technology Industry Association – CompTIA
4. Certified Ethical Hacker International Council of Electronic Commerce Consultants – EC-Council
5. Cybersecurity Fundamentals Educor group
6. Certified Information Security Manager (CISM) Information Systems Audit and Control Association – ISACA
7. Offensive Security Certified Professional (OSCP) Offensive security
8. Microsoft cybersecurity certificate Microsoft
9. Masters in Cybersecurity University of Stellenbosch
10. Penetration testing, ethical hacking, SOC, etc. CREST

Few companies accept matriculants and train them to be cybersecurity officers under the auspices of their skills programme. These companies prefer to teach their employees new skills. Some employers have raised concerns regarding international qualifications that are not vetted. This brings another regulatory challenge as the legitimacy of these qualifications cannot be verified. The appropriateness of training received by cybersecurity specialists is arguably determined by industry standards and requirements. There is, however, no standardised reference material. If one pursues training with one of the internationally recognised training institutions, employers assume that a person has received appropriate training. With this training, employers have certain expectations. Some employers conduct skills evaluations to assess whether a would-be employee has the appropriate training.

4.6 The exclusion of the economically disadvantaged in cybersecurity

Training It will be recalled that before 1994, certain classes of South Africans were excluded from pursuing certain qualifications based on various grounds, including race and gender. These classes of people are the so-called historically disadvantaged persons who became victims of unfair discrimination. In the cybersecurity space, it was found that cybersecurity training can only be accessed by those who are economically advantaged.

Those who possess a certificate, diploma and degree in computer science, criminology, law, or any IT related qualification can only work in certain fields of cybersecurity locally and internationally, provided they are in possession of an additional internationally recognised certificate which comes at a huge cost. This creates a big challenge for an individual who has no means to fund cybersecurity training. The regulation of cybersecurity may provide opportunities for the economically disadvantaged to access cybersecurity training through several interventions, including the introduction of skills programmes for previously disadvantaged groups in the field of cybersecurity.

4.7 The working conditions within cybersecurity

Button (2020, p. 43) emphasised that cybersecurity officers, and in particular moderators, share common traits with physical security guards such as low pay, high labour turnover, and having to deal with incidents that take a psychological toll on them. Contrary to this assertion, the study found that cybersecurity officers are well taken care of, and their rights are respected. Since there is a shortage of cybersecurity specialists, employers treat them well, including paying them well.

After all, cybersecurity is not confined to a certain geographical location, and cybersecurity officers can find a job anywhere in the world. Cybersecurity is internationally marketable. As Button (2020) observed, cybersecurity companies must deal with high labour turnover. In the case of senior ethical hackers who are not more than 30 in South Africa, and must serve a lot of clients, the chances of them not staying for long with one employer are high.

Due to the nature of their work, there is also a high turnover of MSSPs, especially the ones that work at cybersecurity operation centres. These are always working indoors monitoring signals from the deployed technology for 24 hours and 7 days a week. The difference between cybersecurity officers and other employees is that they do not have trade unions. The working conditions of CSSPs are informed by the Basic Conditions of Employment Act 75 of 1997, meaning that they have the same employment rights and benefits as any other employees in the country.

Most CSSPs use normal business hours, which are from 08h00 to 17h00 - Monday to Friday. The exception is in relation to officers who provide managed security services because they work a 12-hour shift. There are no research studies on the working conditions of cybersecurity officers, which points to the need for studies to be undertaken in this area.

4.8The need for regulation of cybersecurity services

According to Button (2020, p. 50), “there is clearly a regulatory gap when the new private security industry is considered”. The study found that cybersecurity services are generally unregulated. There is a need for the regulation of cybersecurity in South Africa. This part focuses on the importance of regulating the new private security industry. The regulation of the new private security industry is possible and the PSIR Act is relevant in this regard. While there are mixed views on the need to regulate the new industry, the study on the regulation of cybersecurity services in South Africa could not have been better timed. Owing to the demand for cybersecurity, existing PSSPs are likely to transform their businesses to offer cybersecurity services.

The private security industry sells “trust” to its end-users, which are clients, and if this trust is compromised, there is an inevitable loss of business. Before a client appoints a CSSP, assurance must be guaranteed on whether a prospective CSSP would have capabilities to safeguard and to respond to alerts in a timely and efficient manner. Therefore, the lack of regulated minimum standards creates an unfortunate “conducive environment” for incompetent service providers to operate in this space.

It is for this reason, among others, that registration requirements (including minimum qualifications) are needed before a cybersecurity company and/or officer can be deemed as such. The nonexistence of regulations results in many companies seeing cybersecurity as a business opportunity in their profit maximisation drive. This compromises professionalism in this space. This also introduces accountability challenges. CSSPs underscored the need for a designated regulator to provide oversight to their operations.

The regulation of cybersecurity services and their providers will always be beneficial to the industry and the citizens in general. It is important to note that where there are regulations in place, professionalism is guaranteed. The nonexistence of specific regulations for cybersecurity services and their providers is also a weakness that cybercriminals have observed, and they are taking advantage of it. Many crimes occur in cyberspace, some of which are created by the fact that CSSPs are not regulated. There are also concerns relating to the issue of standardisation of cybersecurity services and the lack of quality services rendered thereof. It was found that there is huge uncertainty about the quality of services that CSSPs render to their clients.

There are some CSSPs that provide substandard services to their clients and the latter would not be able to pick this up. They only rely on word of mouth on which CSSP can provide the service. The existence of regulations would ensure that the company is accredited and can provide quality services. There are also international best practices and associations found within the industry. However, membership in these associations is voluntary and the best practices are not legally prescribed.

Therefore, clients cannot always rely on whether a company is accredited by a voluntary institution. The need for regulation cannot be overemphasised to ensure the quality of services rendered in cybersecurity. By way of example of the standardisation of services concerning the rendering of cybersecurity services, in the case of penetration testers, some penetration testers charge clients ridiculous amounts for one service.

Their clients would pay because they need work done at a lower cost and overlook the work offered being substandard. Most clients that are not technically savvy do not have the capabilities of determining whether a penetration testing company will provide quality service. In the process, clients lose money as they are sometimes forced to contract another company to redo the work. Regulations become important in avoiding the use of unprofessional service providers.

The regulation of the new private security industry is important as there may be a possibility of industry opting for self-regulation, which may not necessarily be in the interest of the country. The formation of associations for purposes of self-regulation has its pros and cons. The main pro is that the industry arguably subjects itself to some form of control albeit not legally enforceable. In the case of cybersecurity, for instance, the associations would set and/or determine accreditation requirements for CSSPs.

In the UK, there is an organisation called CREST, which is a non-profit accreditation and certification body that represents and supports the technical information security market (CREST, 2021). CREST provides internationally recognised accreditations for organisations and professional level certifications for individuals providing penetration testing, cyber incident response, threat intelligence and Security Operations Centre (SOC) services (CREST, 2021).

a CSSP is deemed by CREST to be fit and proper, most organisations feel safe to appoint CREST accredited companies because they have the knowledge that these providers went through rigorous tests before obtaining the certification. In South Africa, most banks hardly hire people or companies who are not CREST certified. CREST attempted to regulate CSSPs operating in South Africa but was met with resistance from the industry.

Without regulations, the country’s security will be compromised, and associations will emerge to seek to “regulate” the new industry. As part of the regulatory regime, the designated regulator must accredit different cybersecurity training offered by CSSPs. Cybersecurity training institutions must be regulated. There is also a likelihood that cybersecurity training institutions attract candidates from all over the world. Regulation of these institutions, including accrediting their training courses, will professionalise the industry. With the high level of unemployment in South Africa, it is hoped that this new private security industry will create employment opportunities, particularly for the South African youth.

One of the challenges envisaged in regulating this new industry is that most CSSPs operate in the digital world or space where they work remotely and where geographical restrictions are minimal. A cybersecurity company from anywhere in the world, for instance, can render a cybersecurity service to a South African-based company. In this way, certain categories can be effectively regulated in the country and also some cannot be easily regulated. It is more practically possible to regulate CSSPs in South Africa than those outside the South African borders.

The viability or otherwise of regulating foreign cybersecurity companies rendering security services in South Africa remains to be seen. As cybercrime and security measures change now and again, the regulation for cybersecurity needs to adapt to these changes. It is important to note that regulating the new industry will be informed by the dynamics and intricacies involved in this world of cyberspace. Such regulation cannot be an overnight project. While it may seem impossible, it is nevertheless achievable.

CHAPTER 5

RECOMENDATIONS AND CONCLUSION

5.1. Introduction

This chapter presents the conclusion to, and recommendations based on this study by focusing on the categorisation and verification of the study the objectives. of this study.

5.2. Recommendations

From this study, arguably has a mandate to regulate the newly emerged private security industry. It is recommended that a legal opinion is solicited in order to determine the question around the legal mandate of in regulating this industry. If established that the Authority has a mandate, cybersecurity services and its providers will have to be effectively regulated. This means the Authority will have to strengthen its efforts to regulate the cybersecurity industry, including bringing awareness to the public of its legal obligations towards the cybersecurity industry.

This could involve a possible amendment of the current or the development of regulations specifically focusing on the cybersecurity industry. Cybersecurity Training Providers rendering cybersecurity services within, or outside South African borders must be registered. This also includes providers that are not necessarily based in South Africa but provide cybersecurity services in the country.

It is recommended that for purposes of effectively regulating the cybersecurity industry, should categorise the security services rendered in “cyberspace”. Service providers registered as PSSPs should only offer cybersecurity services once they also register. The regulations must be meticulously drafted to regulate this new cybersecurity industry. It would be critical for the Authority to establish a committee representing all the operational divisions that will be focusing on the development of these regulations.

As the current grades are not in line with cybersecurity training, the Authority should consider aligning its training standards to accommodate those offered in cybersecurity. This will also include the accreditation of these standards. In line with its functions, the Authority must also consider developing cybersecurity training courses for CSSPs and prospective CSSPs. The Authority will have to apply to the South African Qualifications Authority (SAQA).

5.3. Conclusion

Cybersecurity, the new private security industry, has emerged alongside the traditional private security industry and is here to stay. Cybersecurity is arguably a security service in terms of the and must consider to be subjected to regulation by the Authority. The need for government to rethink and strategise on how to effectively regulate the cybersecurity industry in South Africa cannot be overemphasised.

The regulation of the industry can only be effectively regulated provided its intricacies are well understood by the Authority. This study highlighted that the nature of criminal activities found in cyberspace, such as malware and ransomware, necessitate new security services in protecting cyberspace. These new services are different to those found in the physical space. Many security services under the auspices of cybersecurity are technology-driven due to the nature of cyberspace, which is intangible or rather digital. The most used cybersecurity measures are intrusion detection systems, firewalls, anti-viruses, and other anti-malware software.

REFERENCE

Abu-Taieh, E.M., 2017, November. Cyber Security body of knowledge. In 2017 IEEE 7th International Symposium on Cloud and Service Computing (SC2) (pp. 104-111). IEEE.

Agarwal, H. and Agarwal, R., 2017. First Industrial Revolution and Second Industrial Revolution: Technological differences and the differences in banking and financing of the firms. Saudi Journal of Humanities and Social Sciences, 2(11), pp.1062-1066.

Allen, J., Gabbard, D., May, C., Hayes, E. and Sledge, C., 2003. Outsourcing managed security services. CARNEGIE- MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Alqahtani, H., Sarker, I.H., Kalim, A., Hossain, S.M.M., Ikhlaq, S. and Hossain, S.,2020, March. Cyber intrusion detection using machine learning classification techniques. In International Conference on Computing Science, Communication and Security (pp. 121-131). Springer, Singapore.

Atkeson, A. and Kehoe, P.J., 2001. The transition to a new economy after the second industrial revolution (No. w8676). National Bureau of Economic Research.

Bacudio, A.G., Yuan, X., Chu, B.T.B. and Jones, M., 2011. An overview of penetration testing. International Journal of Network Security & Its Applications, 3(6), p.19.

Bertrand, C. and Bourdeau, L., 2010. Research interviews by Skype: A new data collection. method. In Paper Presented at the Proceedings of the 9th European Conference on Research Methodology for Business and Management Studies, Madrid, Spain.

Button, M., 2020. The ÒnewÓ private security industry, the private policing of cyberspace and the regulatory questions. Journal of Contemporary Criminal Justice, 36(1), pp.39-55.

Constitution, S.A., 1996. The Constitution of the Republic of South Africa.

Craigen, D., Diakun-Thibault, N. and Purse, R., 2014. Defining cybersecurity. Technology Innovation Management Review, 4(10).

CREST, 2021. CREST - Assurance in Information Security. Crest-approved.org. Available at:
https://crest-approved.org/ [Accessed 19 December 2021].

Cybercrime Act 19 of 2020. Available at: https://www.gov.za/sites/default/files/gcis_
document/202106/44651gon324.pdf

De Vries, J., 2013. European Urbanization, 1500-1800. Routledge.

Deane, P.M., 1979. The first industrial revolution. Cambridge University Press.

Ding, W., Yurcik, W. and Yin, X., 2005, December. Outsourcing internet security: Economic analysis of incentives for managed security service providers. In International Workshop on Internet and Network Economics (pp. 947-958). Springer, Berlin, Heidelberg.

Direnzo, J., Goward, D.A. and Roberts, F.S., 2015, July. The little-known challenge of maritime cyber security. In 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA) (pp. 1-5). IEEE.

Dlamini, S. and Mbambo, C., 2019. Understanding policing of cybercrime in South Africa: The phenomena, challenges and effective responses. Cogent Social sciences, 5(1). p. 1675404.

Dubois, J. and Jreije, P., 2006. Mechanisms of internet security attacks. Transactions on Engineering, Computing, and Technology, pp.166-168.

Electronic communications Act 36 of 2005. Available at: https://www.gov.za/sites/default/files/gcis_document/201409/ a36-050.pdf (Accessed: 09 December 2021).

Electronic Communications and Transactions Act 25 of 2002. Available at: https://www.gov.za/sites/default/files/ gcis_document/201409/a25-02.pdf

Fox, S.J., 2016. Flying challenges for the future: Aviation preparedness–in the face of cyberterrorism. Journal of transportation security, 9(3), pp.191-218.

Furnell, S., 2003, July. Cybercrime: vandalizing the information society. In International Conference on Web Engineering (pp. 8-16). Springer, Berlin, Heidelberg.

Gollin, D., Jedwab, R. and Vollrath, D., 2016. Urbanization with and without industrialization. Journal of Economic Growth, 21(1), pp.35-70.

Harper, M. and Cole, P., 2012. Member checking: Can benefits be gained similar to group therapy. The qualitative report, 17(2), pp.510-517.

International Civil Aviation Organization., (2021). Civil Aviation Cybersecurity. Available at: https://www.icao.int/ cybersecurity/Pages/default.aspx (Accessed: 1 July 2021).

Janicke, M. and Jacob, K., 2013. A third industrial revolution. Long-term governance for social-ecological change, pp.47-71

Johnson (2021). Worldwide digital population as of January 2021. Statista. Available at: https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=How%20many%20people%20use%20the,the%20internet%20via%20mobile%20devices (Accessed: 19 May 2021).

Jones, S.L., Collins, E.I., Levordashka, A., Muir, K. and Joinson, A., 2019, May. What is 'Cyber Security'? Differential Language of Cyber Security Across the Lifespan. In Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems (pp. 1-6).

Kolb, M., 2018. What is globalization: And how has the global economy shaped the United States. Peterson Institute for International Economics. Available at: https://www.piie.com/microsites/globalization/what-is- globalization (Accessed on: 5 July 2021).

Landreneau, K.J. and Creek, W., 2009. Sampling strategies. Available at: http://www. natco1.org.

Lewis, J.A., 2006. Cybersecurity and critical infrastructure protection. Center for Strategic and International Studies.
Mathias, P., 2013. The first industrial nation: The economic history of Britain 1700–1914. Routledge.

Mazzotta, G., 2018. Toward live memory forensics for malware identification.

Mchunu, V., 2021. Cyberattack threatens SA's national security. Available at: https://www.iol.co.za/mercury/news/cyberattack-threatens-sas-national-security-5903bc24-5bbd-483e-a46e-17c080490633 (Accessed: 09 November 2021).

Minnaar, A. and Ngoveni, P., 2004. The relationship between the South African Police Service and the private security industry: any role for outsourcing in the prevention. of crime? Acta Criminologica: African Journal of Criminology & Victimology, 17(1), pp.42-65.

Mohurle, S. and Patil, M., 2017. A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science,8(5),pp.1938-1940.

Nadikattu, R.R., 2020. New Ways of Implementing Cyber Security to Help in Protecting America. Journal of Xidian University, 14(5), pp.6004-6015.

Oppliger, R., 1997. Internet security: firewalls and beyond. Communications of the ACM,
40(5), pp.92-102.