DEVELOPING A FRAMEWORK FOR EFFECTIVE CYBER SECURITY TRAINING IN SOUTH AFRICA

FOR

MDUDUZI ERIC ZAKWE
Student Number: 64876012

DISSERTATION TOWARDS THE FULFILMENT OF DOCTOR OF PHILOSOPHY

in the subject

PHILOSOPHY STUDIES

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISORS:

PROF SA NGUBANE
DR B MANYONGA

March 2023

DECLARATION

By electronically submitting this research thesis, I, Mduduzi Eric Zakwe, certify that all of the content is my original, original work, that I am the owner of the copyright thereto (unless expressly stated otherwise), and that I have not previously submitted it in whole or in part for the purpose of obtaining any qualification.

Mduduzi Eric Zakwe

ACKNOWLEDGEMENT

All glory to God Almighty, who gave me the fortitude to endure the storms when it seemed impossible to take even a single step and finish this piece of work. May He continue to guide me and channel my passion in offering cyber security education.

I also like to thank the following folks that helped this study be completed successfully.

- Prof SA Ngubane who provided guidance and nurtured my research capabilities. She was passionate about the field of education and this study matched her passion. Her insight on shaping the direction of the study was invaluable, particularly to someone who came from corporate.
- Dr. B Manyonga offered guidance and great insight on the current education landscape and in particular developmental agenda and the need for our education offering to remain relevant to our current times and in preparation for future leaders.
- Survey respondents who took their time to complete research survey forms and sit on interviews. I will always be grateful for their encouragement and wisdom.
- My late Grandmother Mrs. Lephinah Zakwe, who was my best friend, with whom we shared mutual respect about our choices in life and always assured me that life had so many possibilities if one had the education.
- My family who was supportive and critical of some of the developmental concepts that I was working on during the survey. Their critical viewpoint had impetus on the shape and direction of the study.
- My research assistant, Ms N Zungu, who provided a helping hand in coordinating interviews and meeting confirmations with respondents.

ABSTRACT

The objective of this study was to formulate a roadmap upon which a curriculum for cybersecurity can be built to bring about a resilient cyber-workforce, thereby enabling South Africa to be on par with or ahead of international cybersecurity know-how through a fusion of innovation, research and development that sharpens the country's academic programmes and training. The purpose of this roadmap is to emphasise sustainability strategies relating to policy, capacity, and governance.

A mixed method research design, comprising a design-based approach that was iterative, integrating, flexible, context based, pragmatic and grounded in both theory and real-world contextual situations and a case study approach that complemented the design-based research through the interrogation of real-world contextual situations, was adopted for the study. Purposive sampling with domains of exploratory, descriptive, and inductive research was used to support the case study approach. Curriculum development managers, lecturers and managers of the Media, Information and Communication Technologies Sector Education and Training Authority (MICT SETA) were approached to take part in interviews. Owing to the homogeneity of the target population, non-probability convenience sampling was also used for the study. For purposes of qualitative research, interviews were conducted to collect meaningful content, a survey questionnaire was administered to randomly sampled research respondents and online surveys were administered to purposefully sampled respondents for the quantitative triangulation of data.

The results of the study revealed that there is a great need for cybersecurity skills to guarantee the country's cyber liberty. South Africa lacks resources, expertise, and governance processes, and this is hindering institutions' readiness to prioritise educational programmes on computer security (CS) in response to unabated cyberattacks and rampant cyber espionage. This has systematically produced less cybersecurity professionals while the demand for skills in cryptography, secure coding, penetration testing, digital forensics, network security and cybersecurity risk management, among other things, continues to increase. The results of this study also highlight a need for coherent thinking that pulls legislators, policymakers, researchers, innovators, and educators together to plug the security holes, to ease institutional rigidity and to tackle the lack of depth and breadth in South Africa's CS offering. The inadequate CS offering has caused multinationals and other private sector stakeholders to import or train their own talent, leaving the public sector with a shortage of cybersecurity skills

The recommendations made based on the findings of the study include the elimination of restrictive practices that work against innovation, on the one hand, and the promotion of cybersecurity investment and outside collaboration, on the other. Capacity governance, according to the model proposed in the study must augment the Cybercrimes and Cyber Security Bill which does not adequately address the cybersecurity skills agenda. The government needs to adopt medium to long-term policies that will create a sustainable supply of cybersecurity professionals in academia and industry. South Africa should embark on large-scale CS awareness-raising and public education on the importance of cybersecurity through, for example, cyber-hygiene campaigns that target different demographics of its cyber-citizenry and effect meaningful change in academic settings and hiring practices. CS courses must be introduced from the primary and secondary levels to the tertiary and postgraduate levels. Inter-institutional cooperation will be vital since we are all fighting the same adversaries in the cyber-terrain. The use of shared laboratories and simulation laboratories must be explored as a possible means of creating the resources needed to bring about a competitive CS offering. Training will be vitally important in creating champions of change in the fields of justice, law enforcement, academia, research and policy formulation. In the interest of delivering impactful education and cutting-edge resources, well-funded research is paramount to building a capable state, stimulating innovation, promoting commercialisation, and reversing the information technology import/export conundrum.

Keywords: Technology, Cyber Security, Cyber security curriculum, Cyber security framework

ISIFINYEZO

Inhloso yalolucwaningo kwakungukwakha umgomo wezindlela zokwenziwa kwezifundo ze-cybersecurity ukwakha amandla okusebenza kwesibhekelele, ngakho-ke kwenza iNingizimu Afrika ibe ngokulingana noma ingaphezu kokwazi kwesibhekelele sezwe lonke ngesihlanganiso sobuchwepheshe, ucwaningo nokuthuthukiswa lokukhiqiza izinhlelo zokufunda nokuzimisela zezwe. Injongo yalomgomo wezindlela wkugcizelela izinhlelo zokuphila ezihlobene nemithetho, namandla nokuphatha. Uhlelo lokucwaninga oluhlanganisiwe, oluqukethe uhlelo lokwakha olubhekene nokucwaninga olubhekene nokuhlanganiswa, ukubeka kabusha, ukunquma, ukusekelwa kwendawo, ukuba nomsebenzi nokuzimisela emazingeni amaningi kanye nokuhlanganiswa kwesimo sangempela namazinga amaningi, kanye nohlelo lwengcwaningo lwe-case study olusekelisana nohlelo lokwakha olubhekene nokucwaninga ngokuhlola izimo zangempela, lwamukelwa kulolucwaningo. Ukutholwa kwamaphuzu okucwaninga okungokuzinikela ngamagumbi okucwaninga okuyizindaba ezihlobene. Abaphathi bezinhlelo zokuthuthukisa isifundo, abafundisi nabaphathi be-Media, Information and Communication Technologies Sector Education and Training Authority (MICT SETA) batholakala beyingxenye yemibuzo. Ngenxa yokufana kwengeniso yomphakathi wokucwaninga, ukutholwa kwamaphuzu okucwaninga okungokuzinikela kwasetshenziswa kulolucwaningo.

Imiphumela yocwaningo ibonisa ukuthi kukhona isidingo esikhulu sezinhlelo zokusebenza kwesibhekelele ukuze kugcinwe inkululeko yesizwe esiyisisekelo. INingizimu Afrika inezinsiza, ubuchwepheshe, nemithetho yokuphatha, futhi lokhu kuyivimbela izikhungo ukuba zibe nesiqiniseko sokufaka isifundo se-computer security (CS) njengobuningi bobandlululo bezinkomba zesibhekelele kanye nobandlululo obunamandla wesizwe esiyisisekelo. Lokhu kwenzeke ngendlela ehambisanayo ekukhiqizeni abasebenzi abancane bezinhlelo zokusebenza kwesibhekelele ngenkathi isidingo sezinhlelo zokusebenza kwesibhekelele ezihlobene nokubhala okuvikelekile, ukubhala okuvikelekile, ukuhlola ukuvikeleka, ukubhalisa okuvikelekile, ukuvikeleka kwamakhompyutha nokuphatha izinhlelo zokusebenza kwesibhekelele, phakathi kwezinye izinto, siqhubeke sikhula. Imiphumela yalolu cwaningo ibonisa futhi isidingo sokucabanga okuhlanganisiwe phakathi kwabaholi bomthetho, abaphathi bezinhlelo, abacwaningi, abaqalisi kanye nabafundisi ukuze kuvalwe izikhala zokuvikeleka, ukuqeda ukungabi namandla kwamakhungo kanye nokulwa nokungabi namandla nokubanzi kokunikezwa kwe-CS eNingizimu Afrika. Ukunikezwa okunganele kwe-CS kwenze izinkampani eziningi ezimkhulu kanye nabanye abasebenzi bezinsiza bazitholele noma bazifundise izinhlelo zabo zokusebenza kwesibhekelele, lapho isizwe esiyisisekelo sishiywe nesidingo sezinhlelo zokusebenza kwesibhekelele.

Izimpendulo ezinikezwe ngokusekelwa imiphumela yolucwaningo ziqukethe ukususa izinhlelo ezivimbayo ezisebenza ngokuphikisana nobuchwepheshe, ngakunye nokukhuthaza ukungena kwemali kanye nokusebenzisana ngaphandle. Ukuphatha amandla, ngokwesimo esiphiwe kulolucwaningo kumele kusekelise i-Cybercrimes ne Cyber Security Bill engenakwazi ukuphatha kahle isihloko sezinhlelo zokusebenza kwesibhekelele. Uhulumeni udinga ukwamukela imithetho emaphakathi esizweni esizokwakha isiqiniseko sokutholakala kwabasebenzi bezinhlelo zokusebenza kwesibhekelele emazingeni aphakeme nasezinkampanini. INingizimu Afrika kumele iqale ngokwethula imibhalo yokwazi i-CS nokufundisa umphakathi ngobalulekile bokuvikelekile kwesibhekelele ngesihlanganiso sobuchwepheshe obuhlanganisiwe obubhekene nezihlobo ezahlukene zabantu abangabasebenzi bezinkomba zesibhekelele bese kushintsha okuqukethwe nokufundiswa emazingeni aphakeme nasezinkampanini. Izifundo ze-CS kumele zifakwe kusukela

emazingeni aphansi kuze kube emazingeni aphakeme. Ukusebenzisana phakathi kwezikhungo kubalulekile ngoba sonke nenkinga yabantu abaningi abangabasebenzi bezinkomba zesibhekele. Ukusetshenziswa kwama-laboratory wokwabelana nokwakha amalabhorari okuhlanganisiwe, kumele kuqaphelisiswe njengendlela engenayo yokwakha izinsiza ezidingekayo ukuze kube khona isifundo se-CS esinamandla.

OPSOMMING

Die doel van hierdie studie was om ’n rigtingwyser te formuleer waarvolgens ’n kurrikulum vir kubersekuriteit ontwikkel kan word om ’n veerkragtige kuberwerksmag te bewerkstellig. Sodoende kan Suid-Afrika op gelyke voet met, of vóór, internasionale kubersekuriteit-kennis wees deur ’n samevoeging van innovering, navorsing en ontwikkeling wat die land se akademiese programme en opleiding verbeter. Die rigtingwyser het ten doel om strategieë vir volhoubaarheid ten opsigte van beleid, kapasiteit en bestuur te beklemtoon.

Vir hierdie studie is die volgende gebruik: ’n gemengdemetode-navorsingsontwerp bestaande uit ’n ontwerpgebaseerde benadering wat iteratief, integrerend, aanpasbaar, konteksgebaseer, pragmaties, en in teorie sowel as werklike kontekssituasies gesetel is, en ’n gevallestudiebenadering wat die ontwerpgebaseerde navorsing aanvul deur die ondersoek na werklike kontekssituasies. Doelbewuste steekproefneming met domeine van verkennende, beskrywende, en induktiewe navorsing, is gebruik om die gevallestudiebenadering te ondersteun. Kurrikulumontwikkelingsbestuurders, dosente, en bestuurders van die *Media, Information and Communication Technologies Sector Education and Training Authority* (*MICT SETA*) is genader om aan onderhoude deel te neem. Vanweë die homogeniteit van die teikenpopulasie is niewaarskynlikheid-gerieflikheidsteekproefneming ook vir die studie gebruik. Vir doeleindes van kwalitatiewe navorsing is onderhoude gevoer om betekenisvolle inhoud te bekom; ’n opnamevraelys aan ewekansige-steekproef-navorsingsrespondente gegee; en aanlyn opnames onder ewekansige-steekproef-respondente gedoen vir die kwantitatiewe triangulering van data.

Die studieresultate het getoon dat daar ’n groot behoefte aan kubersekuriteit-vaardighede is – om die land se kubervryheid te waarborg. In Suid-Afrika is daar ’n gebrek aan hulpbronne, kundigheid, en bestuursprosesse, en dit belemmer instansies se bereidheid om opvoedkundige programme oor rekenaarsekuriteit (*CS*) te prioritiseer in antwoord op onverswakte kuberaanvalle en onstuitbare kuberspioenasie. Dit het sistematies minder kubersekuriteit-kundiges gelewer, terwyl die vraag na vaardighede in kriptografie, beveiligde kodering, penetrasietoetsing, digitale forensies, netwerksekuriteit en kubersekuriteit-risikobestuur, onder andere, steeds toeneem. Die resultate van die studie beklemtoon ook die nodigheid van koherente denke wat wetgewers, beleidsvormers, navorsers, innoveerders en opvoeders saamvoeg om die sekuriteitsgate toe te stop; om institusionele onbuigsaamheid te verlig en om werk te maak van die gebrek aan diepte en wydte in Suid-Afrika se *CS*-aanbieding. Die ontoereikende *CS*-aanbieding het meegebring dat multinasionale maatskappye en ander belanghebbendes in die private sektor hul eie talent invoer of oplei, en sodoende die openbare sektor met ’n tekort aan sekuriteit-vaardighede laat.

Die aanbevelings wat aan die hand van die studiebevindinge gemaak word, sluit in: aan die een kant, die uitskakeling van beperkende praktyke wat innovering teenwerk, en aan die ander kant, die bevordering van kubersekuriteit-investering en samewerking van buite. Kapasiteitsbestuur, volgens die model wat in die studie voorgehou word, moet aanvullend wees tot die Wetsontwerp op Kubermisdaad en Kubersekuriteit, wat nie voldoende voorsiening maak vir die kubersekuriteit-vaardigheidsagenda nie. Die regering moet medium- tot langtermynbeleide instel wat volhoubaar kubersekuriteit-kundiges in die akademiese omgewing en die bedryf kan lewer. Suid-Afrika moet grootskaalse bewusmaking van *CS* en openbare opvoeding ten opsigte van die belangrikheid van kubersekuriteit aanpak, byvoorbeeld deur kuberhigiëne-veldtogte wat op verskillende demografiese kenmerke van hul kuber-burgery gerig is, en moet betekenisvolle veranderinge in akademiese kontekste en

indiensnemingspraktyke bewerkstellig. *CS*-kursusse moet bekendgestel word van die primêre en sekondêre vlakke tot by die tersiêre en nagraadse vlakke. Inter-institusionele samewerking sal deurslaggewend wees, aangesien ons almal teen dieselfde teenstanders op die kuberterrein veg. Die gebruik van gedeelde laboratoriums en simulasielaboratoriums moet ondersoek word as ’n moontlike manier om die nodige hulpbronne te skep om ’n mededingende *CS*-aanbieding te bewerkstellig. Opleiding sal uiters noodsaaklik wees om kampvegters vir verandering te kweek in die regsveld, wetstoepassing, die akademiese wêreld, navorsing en beleidsformulering. Ter wille van die lewering van impakryke opvoeding en indringende hulpbronne, is goed befondsde navorsing deurslaggewend vir die bou van ’n bekwame staat, stimulering van innovering, bevordering van kommersialisering, en omkering van die inligtingstegnologie-invoer/uitvoer-strikvraag.

TABLE OF CONTENTS

List of Figures

List of tables

LIST OF ACRONYMS

AAS	Applied Associate of Science
ABET	Adult Basic Education and Training
ACM	Association for Computing Machinery
AET	Advanced Evasive Techniques
AIS	Association for Information Systems
AITP	Association for Information Technology Professionals
AJIC	African Journal of Information and Communication
AMCIS	America's Conference on Information Systems
API	Application Programming Interface
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
ATM	Automatic Teller Machine
BCM	Business Continuity Management
BGP	Border Gateway Protocol
BOK	Book of Knowledge
BSIMM	Building Security in Maturity Model
CAE	Chief Audit Executive
CBK	Common Body of Knowledge
CCFO	Critical Cros Field Outcome
CEO	Chief Executive Officer
CERT	Cybersecurity Emergency Response Team
CFO	Chief Financial Officer
CHE	Council for Higher Education
CIDR	Classless Inter-Domain Routing
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMMI	Capability Maturity Model Institute
CN	Computer Networking
CPU	Central Processing Unit
CRC	Cybersecurity Response Committee
CRO	Chief Risk Officer
CS	Computer Systems
CSIRT	Computer System Incident Response Team
CSS	Cascading Style Sheets
DBA	Database Administrator
DBMS	Database Management System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSS	Decision Support System
DTPS	Department for Telecommunications and Postal Services
DVMRP	Distance Vector Multicast Routing Protocol
FFIEC	Federal Financial Institutions Examination Council
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation

HCI	Human Computer Interaction
CSHE	Credentials System for Higher Education
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
IAS	Information Assurance & Security
ICMP	Internet Control Message Protocol
ICT	Information Communications Technology
IEEE	Institute for Electrical and Electronic Organizations Engineers
IM	Information Management
IMAP	Internet Messaging Access Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IPT	Integrative Programming & Technologies
ISP	Internet Service Provider
IT	Information Technology
ITF	Information Technology Fundamentals
ITU	International Telecommunication Union
JCSC	Journal of Computing Sciences in Colleges
KSA	Knowledge, Skills & Abilities
LAN	Local Area Network
MICT SETA	Media Information Communication Technology Sector Education Training Authority
MICT	Media Information Communication Technology
MIME	Multipurpose Internet Mail Extensions
MRD	Mission Risk Diagnostic
NCPF	National Cybersecurity Policy Framework
NDP	National Development Plan of South Africa
NGO	Non-Governmental Organisation
NICE	National Cyber Security Education Initiative
NIST	National Institute of Standards and Technology
OAS	Organisation of American States
OECD	Organisation for Economic Co-operation and Development
OSI	Open Systems Interconnection
OWASP	Open Web Application Security Project
PLTW	Project Lead the Way
POPIA	Protection of Personal Information Act
PWC	PriceWaterhouse Coopers
QDA	Qualitative Data Analytics
SAF	Software Assurance Framework
SAMM	Software Assurance Maturity Model
SAQA	South African Qualifications Authority
SETA	Sector Education & Training Authority
SIA	Systems Integration & Architecture
SITA	State Information Technology Agency
SNA	Social Network Analysis
SNMP	Simple Network Management Protocol
SQL	Structured Query Language

SSA	State Security Agency
STEM	Science, technology, engineering, and mathematics
TCP	Transmission Communication Protocol
UDP	User Datagram Protocol
XSS	Cross-site Scripting
ZAR	South African Currency (Rand)

CHAPTER 1

INTRODUCTION AND BACKGROUND

1.1. Introduction

Cyberspace has become irrevocably and intractably linked with how business is conducted. It has become a platform where online economies thrive where trade knows no borders (Anema, 2014). With all its benefits derived by unsuspecting benefactors, other players have other intentions. These players main goal is to exploit the known and unknown vulnerabilities that exist in the cyberspace. What is apparent is that these players are well funded (i.e., premeditated exploitation of cyberspace vulnerabilities) and they can innovate faster than the companies that are meant to protect us on the cyberspace. These players are called cyber gangs, cybercriminals, and hackers, who keep pouncing the cyberspace for different reasons i.e. political, financial, self-affirmation etc (Abraham & Chengalur-Smith, 2011).

Whatever the cause, cybercitizens (being responsible with the use of the internet) appear lax in designing a full and comprehensive response to combat cybercrime (Johnson, 2017). A response can investigate innovation capacity, cyber security curriculum, and trade on cyber goods and services (imports and exports, policy and enforcement mechanisms and capacitating of our flagship institutions looking after cyber agenda).

Despite efforts to create standards and rules to protect computer systems, networks, and information, organizations, businesses, and governments are not immune to cyber-attack. Werlinger, Hawkey, and Beznosov (2009) claim that the issue is that information technology organizations encounter a number of difficulties in addition to standards and guidelines. Among them include a lack of security tools, a lack of security training, a lack of security culture, inaccurate risk assessment, system complexity, and a lack of security training. Organizations, companies, and governments need information communications technology (ICT) security practitioners who are aware of the dangers, according to Werlinger et al..

When it comes to understanding security, the ICT security practitioner must be able to successfully communicate with stakeholders that do not share their goals or worries. Through a sound approach to information security governance, security risk can be monitored, managed,

prioritized, controlled, and reduced (Cleary, 2008). The ability to monitor, manage, prioritize, control, and reduce cyber security hazards can be learned through the information security programs that higher education institutions offer.

South Africa has made some break-through in some aspects of the response through the Department of Justice & Correctional Service which has enacted a Cybercrime and Cyber Security Bill 6 of 2017 to set the tone of our stance against cybercriminals (Burchell, 2009). As a result of this Bill, other organs of State have started capacitating various cyber security centres mainly for reporting and information dissemination by the South African Police Service, Department of Telecommunications & Postal Services and Department of Communications (Chertoff, 2008).

To curb cybercrime the main organs of State are expected to respond and support the Bill i.e. State Security Agency (SSA) and Department of Basic Education and Department of Higher Education have not even published a single strategy to guide the nation, (State Security Agency (SSA), 2015). The SSA has an Intelligence Academy that can collaborate with or even guide other agencies of the state to develop a full-on education strategy for the cyber security domain (SSA, 2015). This inaction is creating a huge gap in terms of our competitiveness with other nations on our quest for our fair share of the growing cyber security industry. It also forces us to be reliant on what is imported, thereby, defeating the very same objective of maintaining our sovereignty (Paulson, 2012). The State Information Technology Agency (SITA) has been granted by National Treasury a passage to even host government sensitive data abroad (SITA, 2017). This seems to suggest that the state cannot innovate and build secure networks and data centres to keep and maintain our sovereignty.

In the current digital era, cyber security training is faced with many challenges and students in higher education are expected to come up with novel ways to contain cyber-attacks (Martini & Choo, 2014). Because of the innovations of the attackers, subjects and top organisations have kept evolving regularly learning institutions are frequently attempting to refresh coursework, (McGettrick, 2013). Today, institutions of higher learning particularly those that appear to have advanced curriculum and infrastructure in the teaching of information technology-related programmes still have issues that add to the curriculum change question in context.

To maintain curriculum relevance and course significance, teachers are as often expected to explore and re-structure ICT security courses. In my perspective, some security courses have changed from concentrating exclusively on hypothetical and theoretical ideas like cryptography to consolidating the spotlight on the system, framework, or web application security (Martini & Choo, 2014).

For South Africa to create capable cyber experts that can ultimately innovate for the next generation, it could be argued that we ought to focus on STEM disciplines. Challenges of a widening gap between exports and imports of hardware and software can largely be addressed by facing the STEM deficit head-on and creating the right calibre of scholars and the cyber workforce. This may nurture a STEM society or a way of life that denotes the importance of a nation that has great abilities to solve technical problems and apply STEM to create and use new knowledge to seize these market opportunities (Caldwell, 2013). Furthermore, STEM deficiency will reduce the ability to build the right calibre of ready and able scholars and professionals who can address threats and security weaknesses and be able to deal with cybercriminals. Pricewaterhouse Coopers (PwC) mentions that the determination to fight for market share will be a lost cause if we do not address STEM deficiency of education system but also curriculum content that considers the changes in the Cyber security landscape (PwC, 2015).

South Africa is ranked as the most cyberspace attacked country in Africa hence the need for the country to invest in cyberspace education (Turok, 2017). This can take the form of short courses, awareness programmes or accredited qualifications or gamification (Assante & Tobey, 2016) An educated and cyber aware workforce can be a very useful component in building cyber capabilities.

In a world that is so deeply interconnected by digital technology, Cyber security and global security become important. This spread of technology has created complex vulnerabilities that may undermine the security of organisations and the country. In South Africa, cyber security has received attention but there seems to be a lack of a competent and adequate cyber workforce hence the need to initiate a discussion on first establishing a cyber-security education framework and influencing course content that is suitable to our development agenda as cited in National Developmental Plan Vision (2030). The education system must be re-engineered to empower individuals, communities, and organisations to disrupt cybercrimes.

1.2. Understanding cyberspace

Technopedia (2010) defines cyberspace as a virtual computer world upon which online communication takes place on the globally interconnected network of computers. Technopedia (2010) further elaborates that cyberspace allows users to share information, conduct business, engage in social forums amongst other things. Because of this dependency, cyber attackers have found a bee-hive of information they can pounce on and commercialise or conduct counter-intelligence or develop advanced persistent cyber shells hence a real need to improve Cyber security in cyberspace.

According to the International Telecommunication Union (ITU, 2010), cyber security is a collection of tools, tactics, security concepts, security barriers, rules, risk management techniques, activities, best practices, affirmation, and innovations that can be used to ensure the association's and client's benefits in the digital environment. Benefits of the association and the client include all connected computing resources, personnel, infrastructure, programs, services, media communications frameworks, and all transferred or possibly stored data in the digital format. With regards to substantial security concerns in the digital world, cyber security aims to ensure the achievement, maintenance, and protection of the security properties of the organization and client's assets (Hsu, & Backhouse, 2012). Additionally, it is clear that the electronic devices, guidelines, security theories, security barriers, rules, risk-management techniques, activities, instruction, and affirmation and innovations have not been successful in fighting cyber or digital offenders and defending data resources (Bishop & Irivine, 2010).

The twenty-first century has witnessed a converged and collaborated online growth through one global network of interconnected computers, the world remains oblivious to the risks faced in the cyberspace. The level of inter-connectedness has grown with the growth of mobile devices and cyber risks have also multiplied through this level of interconnectedness. This trend requires us to rethink the Cyber security agenda through restructuring and redesigning the cyber security curriculum and training to be constantly relevant to cyber risks.

1.3. Problem statement

As a developing nation we are becoming more reliant on the use of information technology in the digital economy and organized cyber gangs are exploiting this opportunity to pounce on unsuspecting citizens. South Africa has suffered immensely from data exfiltration and economic sabotage at the hands of theses cyber gangs. IT Web (2023) , also noted the impact of cyber crime on the South African economy is estimated at R2.2 billion per annum. Many of the security tools we use to protect ourselves are imported with their industry curriculum and skills and regrettably this has helplessly left us on number 8 globally on list of countries vulnerable to cyber attacks (Cybersecurity Insider, 2023). It is also worth noting that South Africa is ranked 5th globally on cyber crime density list (IT Web, 2023).

As much as 3,4 million professionals are needed to fill the cyber security skills gap globally (ISC^2, 2023) while Choo (2018) noted that the Centre for Cyber Safety & Education revealed that there was 1.8 million shortage of Cyber security workforce in 2022. By deduction, the cyber security skills gap increases by 1.5 million globally per year and this cannot be allowed to grow exponentially without a fitting response to improve supply of cybersecurity professionals. With short supply of cybersecurity professionals, we will have less equipped, less educated and less informed computer users that will fall prey to hackers because of their inability to recognize security threats and vulnerabilities unless we revisit the framework for providing cyber security education including supportive strategies like innovation to continuously research and develop better tools. Our challenges are made worse by the fact that businesses find it difficult to find and hire qualified and knowledgeable cyber specialists. Most learning institutions produce Information and communication technology professionals with little or no insights into Cyber security (Irvine, Chin, & Fruickle 2018). So far, however, there has been little discussion about the non-existent cyber education framework, non-existent national Cyber security education strategy, and non-existent coursework at places of higher learning (Kapoor, 2017).

Kapoor (2017), highlight that the issue with cyber security is about lack of exposure to cyber security concepts at the school level, either on computing courses or on embedded subjects; non-availability of simulation laboratories, a complete lack of suitably qualified teachers; the absence of career guidance and counselling; and the growing shortage of current cyber security personnel and under-trained security professionals in both the private and public sector.

This lack of capable cyber workforce is impacting the Department of Justice from policy advocacy, SA Police Service to pounce on cyber gangs with fitting tools and cyber trained & empowered police force, universities, and colleges from continuously re-designing the rigid cyber security curriculum offering and better coordination between government departments especially the security cluster. We have CSIRT (cyber tools or infrastructure) within the Department of Telecommunications and Postal Services, but we get attacked by the same attack variant, a clear indication that public education, tools and infrastructure are not structured and governed and coordinated to protect citizens in the cyber terrain. Creating a capable cyber workforce is a must if we are to protect crown jewels created on the digital economy and restore integrity of our data and systems.

This thesis seeks to understand why hackers have so much advantage in terms of sharpness of their skills and conceptualise and formulate a cyber security framework that could be implemented to build a capable cyber workforce for a protected world. From this framework we could then develop an educational strategy and effect coursework revision. These theses will also fill the gap in the dearth of research on cyber-security education and contribute to a non-existent scholarship on teacher training in cyber security education.

1.4. The purpose of this research

The aim of this thesis is to explore and assess the current state of ICT curricula programs related to cyber security offering in South Africa in relation to the demand of cyber security professionals and investigate fundamental curricula design challenges. The objective is to formulate, design an appropriate cyber security framework, through an explicit and concerted approach to cyber security learning, that can serve as a roadmap for the creation of cyber security curricula for our learning institutions that can assist with the creation of capable and well-equipped cyber security workforce.

This thesis aims to address the following questions through literature:

i) What regulations govern cyber security education in South Africa currently?
ii) Why South African computer security offering is falling short in meeting the demand for capable cyber personnel?
iii) How well equipped are our educators and learning institutions in computer security offering?
iv) How can South Africa's higher education help close the growing skills gap in the cyber security sector by creating a skilled cyber security workforce?

Three sub-research questions will also help to lead this study in addition to the main one:

i) How may a cyber curriculum be built inside the ODL teacher training curriculum to support a variety of security programs/types?
ii) How should a curriculum be structured to cover the main aspects of current market developments in the field of cyber security?
iii) How can the institution promote the alignment of educational initiatives with business demands in the field of cyber security?

1.5 Significance of the study

From scholars to the President of the country, we all suffer from cyber-attacks, data breaches and identity theft. There are many elements that are meant to be part of the fortification of our networks and systems i.e. people, technology and processes, data and systems. This thesis is significant because it recognizes general public concerns of cyber security attacks, and the public can benefit from this research as it explore innovative ways of creating a capable cyber work force that can defend our cyber terrain.

A concerted approach to innovation this research will focus on will be on curricula development and revision, offering or teaching of the cyber security curricula, governance and sustainability. This is critical as it will enhance the outcome of our cyber security offering with capable cyber workforce that can meet the industry demand.

Educators will benefit immensely through this study since they will now be able to equip themselves to be cyber aware and equipped to build on elementary concepts as the learners grow with their curricula.

Policy makers may include the Department of Justice, SA Police Service, State Security Agency, Department of Telecommunications and Postal Services, South African Bureau of Standards, Department of Monitoring and Evaluation. As much as the President has signed the Cybercrimes Bill into law, the bill deals with behavior of those committing unethical and unlawful acts in the cyber space, but the bill is mute on workforce development or curricula or education. As part of better coordination amongst government organs, Justice department would benefit immensely through cyber security policy strategists. SA Police service currently cannot respond to a reported cyber incident because of an ineffective CSIRT and untrained police force on matter of policing cyber-attacks to Her citizens. The SA Police Service as an influencer of education outcomes can benefit from this study in terms of the veracity of types of professionals the new framework can be able to produce i.e. cyber cops, incident responders, cyber guards etc. Department of Telecommunications and Postal Services together with the SA Bureau of Standards can benefit on innovative ways to creating standards in terms of IT gadgets that we import in terms of level of fortification since such we get attacked on the very same gadgets. The Department of Monitoring and Evaluation can also benefit from a governance practice it ought to put in place and implementing that iterative process of feeding back to academia, policy makers, law enforcers in terms of what they monitor in the cyber-attack terrain.

A new model of creating a capable cyber workforce will certainly be appreciated by the job seekers since the industry demands will be matched by their certifications and they will now be equipped with the right tools to perform their roles and responsibilities. A skills gap will slowly be shut by these job seekers.

Academia would also benefit from this research because they would learn the need to put in place practices for the revision of the rigid education curricula. Key initiatives like outside collaboration would benefit academia if conducted correctly. The study evaluates the effectiveness of academic information security programs, considering both current curricula directions and prospective directions for more responsive curricula. In this study, it is indicated what steps should be taken to make university curricula responsive to the needs of the public and the industry in which graduates with specializations in cyber security could find employment. It thus builds on and contributes to the literature on key challenges of Cyber security and how education can contribute to addressing threats and security weaknesses.

Regarding knowledge production by future researchers, there is room to make a real change through bigger sample sizes and factor other critical roles players that are part of the cyber security offering or institutions that can influence or contribute to the development or revision of the cyber security curricular. Future research in the field of ICT (especially cyber security) is an absolute must be due to the dynamic and ever-changing landscape hence new solutions in keeping with the right level of capable cyber workforce would be needed and this can continuously contribute to knowledge generation.

1.6 Outline of the study

The following are the research chapters highlighted:

Chapter 1: Background information, a problem statement, research objectives, research questions, definitions, and limits are all included in the introduction chapter.

• Chapter 2: Literature Review – This chapter will present the study's theoretical framework, which is based on a thorough literature review.

• Chapter 3: Theoretical Framework—In this chapter, the theoretical and conceptual framework for the investigation will be presented.

• Chapter 4: Research Methodology—In this chapter, the research model and methodology will be described.

• Chapter 5: Data Analysis – The outcomes of the data analysis will be presented in this chapter.

• Chapter 6: Proposed Model – In this chapter, the proposed model will be presented, along with a model evaluation.

• Chapter 7: Conclusions– In this chapter, the importance of the study's contribution will be discussed.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This section sets the scene for the study and examines a wide range of information technology-related sources to comprehend the depth of cyber security, including software engineering, designing, political analysis, security, management, education, and human science. As rightly put by Cavelty (2010), there are various interlocking discourses around the field of Cyber security. This section aims to highlight what is already known, the existing gap and how this study can contribute to existing literature. The review is divided into three sections: the first section examines national security concerning Cyber security and it also provides the definition of Cyber security, the second section focuses on demystifying Cyber security in education and the last section looks at course development and maintenance.

2.2. Understanding Cyber security

An analysis of the term Cyber security classifies two spaces of "digital" and "safety" exclusively for conversation and shows a part of heritage. In most higher education institutions, "cyber" is a Network (internet) prefix that means electronic communication and extended reality (Oxford, 2014). It progressed from the articulation 'made by man or artificial intelligence,' which implied the 'control field and the hypothesis of correspondence.'

There is no fully recognized notion on the meaning of the term "security," and the term was generally difficult to describe (Tehan, 2015: Cavelty, 2010). Buzan, (1998) points out that defence, in general terms, requires who securitises, on which issues (risks), for whom (referential challenge) and why, and under which conditions (structure). While there are increasingly strong categories of security (for example, physical characteristics of the organisations, human properties, information system properties or logical meanings for different forms of security), this concept is contrary to a significant point of view. It remains a checked concept and thus a central security law is essentially free of risk. (Oxford, 2014). Regardless of the protection as a topic tested, Baldwin (1997) notes that this role "cannot be used as an excuse for not arranging one's protection as obviously and as efficiently as normal given the current situation."

As a result, these selected definitions of Cyber security that can provide a material perspective of Cyber security entails:

> "Cyber security comprises generally of cautious techniques used to recognize and defeat would-be gate crashers" (Kemmerer, 2013).
>
> According to Lewis (2016), cyber security involves defending PC systems and the data they contain from intrusions and harmful interruptions.
>
> "It includes decreasing the danger of pernicious assault to programming, organisations and systems. This incorporates devices used to identify break-ins, stop infections, square noxious access, implement confirmation, empower scrambled interchanges, unendingly" (Bajaj, 2010).

Besides, "Cyber security" is a part of the wider 'information security' discipline. The cyber prefix includes computers and/or networks, but many of the policies and procedures on information protection do not mention computers or networks (Cavelty 2010). In comparison, safety in information applies to all aspects of information security and defence against unauthorized access or use. Regarding the notion of information security and the inclusion of

governance, private and public policy, and legal considerations, information assurance is the most broadly applicable (Kessler & Ramsey, 2013). During this thesis, the words Cyber security and security of information are used.

Cyber hazards and dangers can be both physical and logical, putting cyberspace and the systems that support it at risk. Intelligent cyber actors and national states take advantage of information, cyberthreats, and cyber vulnerabilities to strengthen their capacity to obstruct, terminate, or jeopardize the delivery of essential services. Nowadays, a wide range of common crimes are perpetrated online. This entails the production and transmission of child pornography and child trafficking conspiracies, banking and financial fraud, infringement of intellectual property, or other crimes with serious human and economic repercussions.

The following are some of the reasons why, according to Bajaj (2010), cyberspace is challenging to secure:

• The ability of malicious actors to operate from any location

• The connections between cyberspace and physical systems

• The challenge of reducing vulnerabilities and consequences in complex cyber networks.

The following vital infrastructures are increasingly concerned with cyber threats

- Chemicals storage facilities;
- Communications towers;
- Dams & reservoirs;
- Energy & distribution lines;
- Food & agriculture;
- Health & environmental health;
- Nuclear plants;
- Government facilities;
- Information technology;
- Transportation systems;
- Commercial facilities;
- Vital manufacturing facilities;
- Industrial defense foundations;
- Emergency services;
- Financial services;
- Government facilities;

- Nuclear plants; and
- Materials

These industries are subject to sophisticated cyber breaches, which adds new dangers. There is an increased possibility of large-scale or high-impact incidents that could harm services or disrupt people's lives and hence disrupt the economy as IT is gradually integrated into physical infrastructure operations.

Because of the possible danger and implications of cyber incidents, improving the protection and resilience of cyberspace has become an important domestic security mission (Kessler & Ramsey, 2013).

Like any technological advancement in history, there will always be people who use such advancements to their benefit as new possibilities are generated (Kessler & Ramsey, 2013). Despite viruses and malware threatening our cyber liberties since the advent of computing, knowledge of computer system safety and the holiness of data has gained momentum before the explosion of the Internet, which has provided hackers with a real sandbox to test their skills by revealing so many machines on the web – denying access to websites, exfiltrating data or conducting cyber espionage and fraud. It’s all that they call cybercrime today.

Since then, the likelihood of cybercrime has increased dramatically due to the projected 3,4 billion internet users (or around 46% of the world's population). A multidisciplinary approach is being used to combat this, involving hardware, software, organizations, and individuals, all of whom are working to either prevent or lessen cybercrime. This activity relates to cyber security.

There is no magic bullet; Cyber security is a continuously changing and constantly active mechanism just as it is aimed at preventing threats. What happens if security is compromised? As the Ashley Madison hack openly showed, security has failed for the majority of trusted internet activities lately, particularly on account theft and the disclosure of usernames and passwords that result in financial gain or the loss of confidential company or government information. This level of compromise if further illustrated in figure 1.1 below where various vectors of compromise are explained.

One reality remains clear, it can only expand. As technology continues to be incorporated into our lives, harassment opportunities are growing. Also, the protections employed must avoid them by Cyber security education and practice.

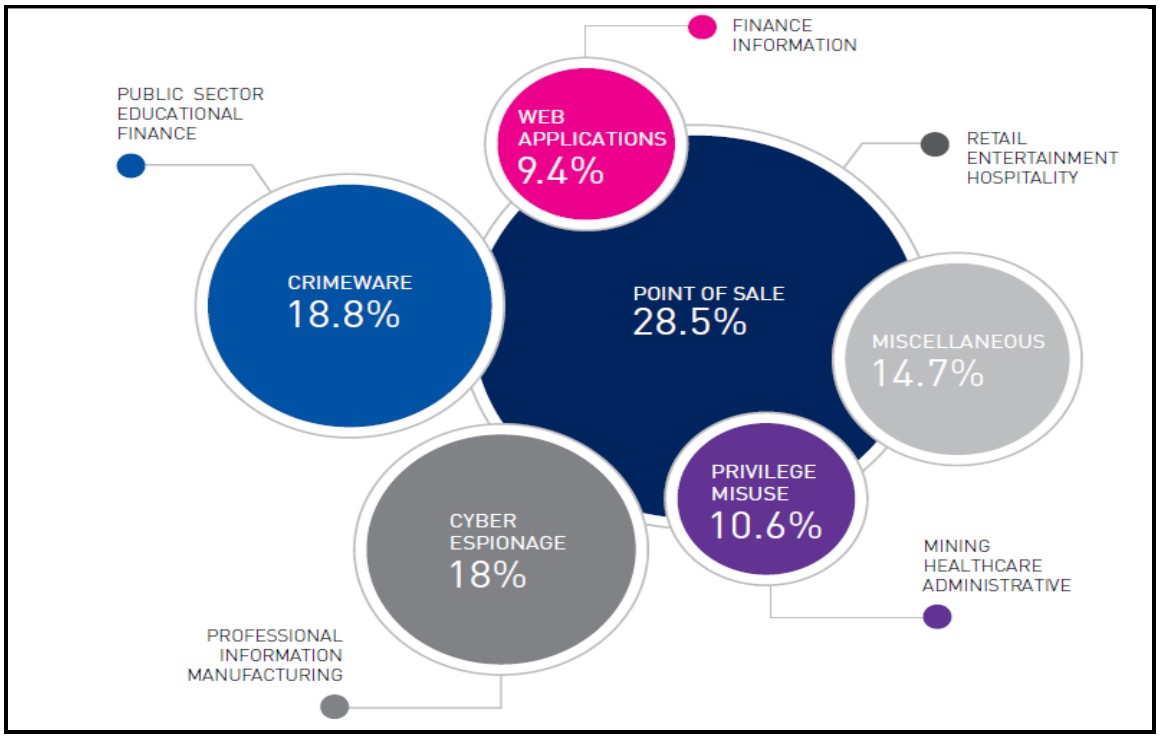

Figure 2.1 The methods used to compromise industries. *Source: (Verizon, 2015)*

Infrastructure is one of the most harmful objectives for a society involved in cyberwarfare. The emphasis on automation concentrates on single points of failure that, if targeted at power plants, communication networks, transportation, and other utilities, can have disastrous effects (Verizon, 2015).

2.2.1. Cyber security scope

The term "Cyber security" has two possible spellings: some people spell it as one word, while others spell it as two words. As a result, this is the primary difference among all respondents in the cyber security community, which may be closed by agreeing on a single spelling.

.

Practices	
Technology	Process
DATA	
Software OS, Dbase, Programing language	
Hardware Servers, PC, PDA, storage, switches	
Network Wired & Wireless	

Figure 2.1 Cyber security elements *Source: (Verizon, 2015)*

As a result, this portion of the chapter summarizes the various discussions about the definition of the phrase "Cyber security." A framework of elements is given in the scope section to at

least limit the invasions of certain irrelevant concepts. Additionally, Figure 1.2 above from this section demonstrates the components of the cyber security framework.

The ability to stop or defend the usage of cyberspace from cyberattacks must be defined as cyber protection, which also includes cyber defense (Bialaszewski, 2015:29). However, Brown and Wang (2014) conducted a thorough investigation in 2014 to clarify the word's ambiguity. The chapter's authors identified nine distinct definitions for this situation, and the tenth definition, known as "Craigen's definition," is as follows: "Cyber safety is the organization and selection of tools, processes, and mechanisms used to prevent situations which misalign the de facto rights of property." Cybersecurity refers to the protection of systems that use the internet and the internet itself.

The definition's three components—security, which refers to activities, technologies, and processes, and includes definitions of internal and external/hostile or naive dangers and attacks—drive one another. The definition's three components include hardware, software, networks, and data, among other things. The different attacks in this area are based on technology and its development, hence the means of defense depend on technology and how attacks are handled, creating a vicious cycle (Brown & Wang, 2014).

2.2.2. Cyber Security professional and Talent Gap

Marisa Vivieros, vice president of IBM Corps, discusses the results of a new analysis by the United Kingdom's National Audit Office in the 2013 Harvard Business Review article "Cyber security relies on education." The study emphasizes that it takes up to 20 years to cope with the skill shortage, not just the available pool of security-educated graduates and working experts are out of demand (Viveros, 2013). Viveros points out that higher education, on-the-job preparation, and training are essential to the growth of the workforce, but that secondary education is not listed. When high school students graduate, they may lose the chance to involve students with a variety of options. Viveros argues that systemic solutions are part of a holistic crisis. Educational agencies adopt interdisciplinary approaches and organisations can adopt those approaches (Viveros, 2013).

Frost and Sullivan's Global Information Security Workforce Studies "2015" have been established in collaboration with the International Information Systems Certification Consortium (ISC^2), (a non-profit organisation which specializes in information security

education and accreditation); Booz, Allen, Hamilton; NRI's Safe Technologies Management Consultancy Corporation; this thesis stresses the need for more security workers and claims it is directly linked to the above-mentioned violation reports and presidential guidelines. This White Paper concludes that a lack of security personnel increased in 2014 compared to 2013. This deficit was attributed not to budget constraints, but to insufficient pool of appropriate information security guidelines. The statistics was compiled which revealed a quantitative shortage of nearly 14,000 people worldwide. The study predicted that in [2015] there was a need for 195,000 cyber-security personnel and, when aggregated annually, the number was going to hit 1.5 million in five years [2019] worldwide. They specifically attributed this to the continuing evolution of the diversity and complexity of cyber-attacks and the widening of the footprint requiring security surveillance, primarily smartphone, cloud, and the Internet. The need for more qualified staff, stronger security priorities and more efficient end-user training (Frost & Sullivan 2015).

Over the past 5-10 years, data security positions and job titles have grown. Survey respondents from Frost and Sullivan put most in-demand security analysts, followed by security auditors; security architecture (products, solutions); forensic analysts; security engineer (applications); security engineers (planning, design); network security; security testers; security system administers; security engineers (platform); security policymakers; security architects (consultants). Software architects and professional experts, as well as managers, are required. The top five positions of leadership include chief security officer, director of information security, chief information assurance officer and quality assurance manager, and chief security engineer (Frost & Sullivan, 2015).

The study includes comprehensive statistics on individual employment, vertical market, workers' projections, and weaknesses, but does not deal with schooling as a response to inequality between employees. The white paper proposes a training approach be adopted and kept. Overall, the study reflects on the behaviours and expectations of IT staff (Frost & Sullivan, 2015).

One of the shortcomings of this White Paper is that there is a quick generalization of the risks and benefits of a career in information security only at the end of the study. The report notes that knowledge needs to be increased not only in the information technology sector but also among future IT specialists, many who are still studying among the many qualities academic institutions planning to join the workforce of tomorrow. The lack of information security specialists can only be solved honestly by recruiting more [students] to the security profession (Frost & Sullivan, 2015).

The Ponemon Institute is an information management, privacy, and data protection research centre. The "Understanding and at Risk: Today's IT Security Service" study report from 2014 cites the lack of a team of security professionals who can handle various and serious internal and external hazards to the firm as one of the major barriers to a successful security posture. Hewlett Packard (HP) Corporate Security funded the study to clarify the present position of the IT security systems of today. It focuses on the attraction and retention of qualified IT security personnel by organisations (Ponemon Institute, 2014).

Since 2012, several things have changed and/or raised the demand for professional IT security personnel in the following manner:

- The number of open positions due to the difficulty in hiring qualified candidates.
- The duration of employment and the issue of excessive turnover, particularly among the more experienced security practitioners.
- Payroll benefits that may not be sufficient to recruit and retain employees.
- The qualifications and backgrounds that security personnel find most appealing (Ponemon Institute, 2014).

The statistical quality of the surveyed included 504 United States human resources and IT security specialists. To ensure a competent respondent, only the persons in charge of attracting, employing, supporting, and sustaining IT security workers in their organisations were eligible to complete the survey (Ponemon Institute, 2014).

The IT security function is understaffed, according to the main findings of this study. According to 70% of respondents, organizations do not have enough IT security personnel.

- It is anticipated that by 2014, there would be 29 employees on average working in IT security functions, up from 22 in 2013.
- In 2013, senior staff roles in IT security went unfilled at a rate of 58% on average. The percentage of open positions is predicted to fall to 49% in 2014, and respondents were confident that the employment of senior IT security specialists will improve.
- Senior security managers don't hold their jobs for very long. CISOs and those in comparable positions typically quit their jobs after 2.5 years. The average tenure of a technician or similar position is four years.
- Human resources and corporate IT are most likely to decide on IT security staffing and hiring.

When choosing a security practitioner, professional certifications, and on-the-job experience matter most. Most of the hiring happens at conferences. Salary is by far the most crucial component of a hiring package. Offering competitive pay can reduce or stop turnover (Ponemon Institute, 2014).

While the number of jobs left unfulfilled and the workplace vacancy rate rose [in 2015], it was projected that the number of vacancies would rise. The study indicates that calls for IT security experts have not been met. The vacancy rate rose by 32% to 36% according to the historical average. In the next years, it will typically increase by 40%. The amount of senior security positions that remain unfilled indicates that organizations are unable to fill these positions.

However, the vacancy rate in the coming year [2015] is decreasing marginally (Ponemon, 2014).

Jontz (2015) points out that "there is an enormous agreement among cyber practitioners that the job force needs considerably skilled workforce, not just the capacity for demand in the coming years" (Jontz 2015, para. 1.) in "Learning of Tomorrow's Cyber Gurus" published in Signal Magazine.

Additional funding and an emphasis on educating youth in computer science and Cyber security were given to government organisations and non-profit organisations. Sandia National Laboratories operates many programs providing computer science and data security instruction through government-wide, academic, and high school educational partnerships. The Cyber security centers are an internship program that puts together students from graduates, students, and high schools on campus over the summer for several months. The team focuses on analysis and experiments on cyber exercises in the physical world. The Cyber Technologies Academy has the aim of early transforming this cyber pipeline to secondary school education. In 2014, a one-week intensive teacher boot camp program was attended by former Catalan computer science teacher Kinnard (2015) of Indianapolis-based Project Lead the Way (PLTW) to obtain an understanding of the student's curriculum.

Curriculum in computer science as published by Kinnard (2015) for all grades and a data security secondary course. To answer the fears of students who might abuse their current experience in addition to teaching technological ability, the course would concentrate on cyber theory and real-life learning PLTW also provides cyber-related lessons at any stage, in addition to the cyber-specific curriculum. Curricula for primary students rely upon cyber hygiene, such as sound password creation; data online security; and web browsing protection. We are now seeking to incorporate [in] general computer science in the middle school level according to

Kinnard (2015:9). It's very hard to reform the education system here in this world, but it's very hard to change in the middle school. The program is still jampacked in most middle schools, so it's impossible to do anything additional "(Kinnard as quoted in Jontzen 2015:10-11).

2.3. International perspective on Cyber security curriculum

As part of national capacity building initiatives, skills growth and curriculum research, multiple facets of Cyber security education have been discussed. The US Homeland Security Service, NIST, the Unites States Nation Security Agency, the UK Government Communications Headquarters, the United Nations, and European Union think tanks all provided in-depth reports on issues pertaining to both the lack of Cyber security professionals and improvement measures in developing economies. However, the amount of research that focuses particularly on comparable problems in industrialized nations is limited.

For instance, the United States of America has enacted legislation and measures for Cyber security education and workforce expansion and views education as a key component of its national cyber security preparation (The World Bank, 2016).

The National Cyber Security Education Initiative (NICE) was developed to strengthen America's long-term Cyber security status (World Economic Forum, 2017). Pleasant works with knowledge, formal schooling, technical preparation, and structure of the workforce. In support of this initiative, NIST created the National Cyber security Workforce Frailty that provides the universities, the business, and the government with a shared language (lexicon and taxonomy). This covers seven Cyber security fields in which provision, work functions and related skills are built by several universities in the United States. These services are often assisted by trained staff (i.e., individuals with extensive data security experience) who are accessible to US educational institutions in the sector. Indeed, RAND's (2014) Education institutions say that they have no issues hiring Cyber security experts amid high industry wages. The United States also struggles to build a Cyber security workforce efficiently (The Organisation for International Co-operation and Development, 2009). A World Bank report noted some concerns on the adequacy of Cyber security activities by staff at work and concerns regarding staff' preparedness to defend IT infrastructure efficiently (The World Bank, 2016)

The teaching and training methods were influenced by the National Institutes of Standards and Technology (NIST, 2019), the NSTISSC (NSTISSC, 2018), and other organizations.

Additionally, the 2002 updates to the 2000 ISO 17799 Information Security Management Standard include incorporate information security education and training requirements.

The NSTISSC (2018) Mandate has laid down a provision for all federal agencies to establish and execute national security systems curriculum, training, and awareness programmes. International Systems Protection Certifying Consortium (ISC) (Percy & Timbs, 2019) identified the essential fields of knowledge CBK which stands for Common Body Knowledge.

But realistic, entry-level talents that are specified in separate standards are what are prioritized. The development of a curriculum based on the NSTISSI principles is also encouraged by the EDACUM software. Some colleges and universities have received accreditation in order to adhere to one or more NSTISSI (2018) requirements. Data on organizations that have been certified by ISA curricula to satisfy such NSTISSI requirements are included in Table 2.1 below. The lowest NSTISSI 4011 minimal requirement is accepted by the majority of universities. No university awards certificates for exceptional skills like system security engineering and risk analysts, which are crucial to every business.

NSTISSI Standard (Year)	**Skill Level**	Number of University
4011 (1994)	INFOSEC Professionals	53
4012 (1997)	Designated Approving Authority	19
4013 (1997)	Systems Administration in Information Systems Security	23
4014 (1997)	Information Systems Security Officers	12
4015 (2000)	Systems Certifiers	7
4016 (in preparation)	Risk Analyst	0
4017 (in preparation)	System Security Engineer	0

Table 2.1 Universities that support various skill categories, as of 2019 (NIST)

Degree/Certification and/or ISA Activity	Number of Universities
PhD with Concentration in IA	7
MS with Concentration in IA	30
BS with Concentration in IA	22
AAS with Concentration in IA	**
Certificate Programmes	22
Research Centers/Institutes	29
Advanced Laboratories	15
Partnerships between Schools	9
Scholarship Offerings in IA	19
Specialized Seminars/Workshops	13
Online Course Offerings	5

Table 2.2. Summary of ISA programmes (NIST, 2019)

** Most two-year college degree programs offer Applied Associate of Science (AAS) degrees.

Various organizations provide certificate programs. Additionally, these credentials only provide a limited amount of experience and skills, and employers do not demand knowledge.

This leads to the recruiting of more employees with different certificates, which contributes to a rise in prices. Higher education institutions must recognize the means to enhance information security education for potential workers in this situation. The study of security education around the world and changes in curricula in universities are important. This segment offers an analysis of education in information security in other countries.

In the United Kingdom, improving electronic defence learning is one of the core four elements of the national cyberspace defence curriculum (2011) (Conti, Babbitt & Nelson, 2011). UK cyber strategy has implemented Cyber security from the age of 11 in all forms of education. Present initiatives include funding schools (for example "Girls get coding"), budget allocation (for example, Open University), literacy programmes, undergraduate and postgraduate study funding, Cyber security job training, and internships. Self-assessment (including academic interviews) to evaluate the challenges of their curriculum delivery in 2013 revealed that existing cyber-education shortcomings need to be addressed in fewer than 20 years (Frost & Sullivan 2015).

The European Commission's Tempus Initiative (2013) examined approaches to formal and informal education as well as public education. While informal education focuses on technical

training and advanced domain preparation (for example, supervisory and data acquisition systems), formal education includes a wide range of Cyber security teaching topics at institutions in the United States, Europe, Asia, and Australia. Public education includes programs for information and awareness. Conclusions show that (i) advanced cyber defense nations like the United States, Canada, the United Kingdom, and Australia implement cyber security training at all educational levels, and (ii) cyber-security education has strong ties to the military and security services, especially in the United States.

In a comparison study between the Czech Republic and Lithuania, Harasta (2013) claims that there is a lack of shared information concerning cyberattacks in both nations. Lehto (2015) conducted an evaluation of education and research in cyber security at 9 universities and study centers in Finland. He describes the approaches and institutional strengths of each institution.

Findings suggest that, while Cyber security education in Finland is improving, there are no systemic priorities in the cyber education framework. Universities offer training focused on unique programmes, collective productivity as well as a robust framework to promote Cyber security studies. Yet institutional Cyber security curriculum programmes should not envisage national strategic capabilities.

The literature covers a variety of facets of cyber safety policy and capacity building among developed countries including cyber education for girls, particular fields of education and regional Cyber security activities. Newmeyer (2015) addresses a national growth's components. Cybersecurity education and awareness are included in policy. Muller (2015) proposes areas in which developed countries are faced with cyber capacity building problems. This include maintaining the institutional framework, increasing public awareness, the regulatory framework, and working with the business sector. As they implement advanced national plans, developing countries should consider their willingness (knowledge, capability, and ability) to carry out strategies quickly (Muller, 2015). Cyber education is briefly stated as a discussion point and a crucial component in protecting cyberspace.

A high-level comparison of U.S. and UK programs in South Africa's national Cyber security strategy establishes the education differences in cyber security in Kortjan and Von Solms (2012). The suggestions include setting up a responsibility allocation schedule, distributing funds, and identifying milestones. A cyber security education program (including a film) for kids is being released by Von Solms and Von Solms (2015) to promote and protect online privacy (including that of social networks). It is emphasized that unlike in Western countries, many African regimes do not typically spend money on this educational activity.

Curbelo and Cruz (2014) discussed the appropriateness and specifications of the university degree in ethical hacking courses in Puerto Rico. The study recommends combining classes on ethical hacking and legal hacking for undergraduate studies. A sophisticated model for Oxford's cyber security capabilities and an online survey, The Inter-American Development Bank, the Organisation of American States (OAS), and the Power Center for Global Cyber Security (2016) provide commentary on the current efforts of 32 nations in five domains, including cyber safety education. Some illustrative educational programs are outlined for each nation. A lack of social consciousness is emphasized as a major issue in this situation, as South Africa largely enters the second stage (i.e., formative) of cyber education (albeit the study's scope does not include any details).

2.4. Perspective on Cyber security curriculum in other parts of the World

The development of ISA curriculum and techniques for implementing curricula in various parts of the world (Canada, Africa, Asia, and Australia) differ significantly. Even though several institutions offer ISA training through standalone courses, the majority of universities include ISA-specific topics as a component of courses on general hardware/software and device architectural topics. Most universities offer postgraduate degrees and master's degrees, including forensic data sciences (Armstrong & Jayaratna 2002, Stevens & Jamieson 2002), Cyber Security Administration, Commerce, Information Security and Data Crime (IPS). Master programmes require a series of security courses for a full-time one year or more for a part-time inscription from 8 to 12 courses. Three areas of knowledge and skill are covered by the themes: general, expert, and practical.

Numerous colleges in Korea offer sound curriculum centered on the fundamental abilities required of those who create and manage information security systems (Kim & Surendran, 2002; Kim & Choi, 2002). Even though the skill sets are largely the same, specialization requirements and program structures vary. Any employer looking to create, implement, and maintain software and information systems as well as their security architecture will find these programs to be a helpful resource. More specific topics relating to schooling are covered in the next section.

In short, most of the associated research focuses on aspects of education as part of building cyber-security, with a greater focus on high-income countries. Finland and the United Kingdom

have a national review of data security education and research in universities. Despite recent attempts to address the potential of cyber defence in less prepared countries, little efforts have been made to recognize unique issues that hinder the creation of national cyber capacities. Therefore, the goal of this study is to acquire a greater understanding of the environmental issues facing a specific developing nation in terms of cyber security education.

2.5. Demystifying Cyber Security in Education

After the definitions, the expression " Cyber security" symbolizes the security of electronic frameworks in which information and data reside. The educating, teaching, and learning of security ideas are not unique yet happens to be increasingly fitting during the 1980s. In 1986, Forcht acknowledged a few explanations about training and industry where security ideas were concerned. She asserts that:

> “Teachers and instructors have since contested with the issue of whether to disregard the data security issue to decline opening a "Pandora's Box" or whether to go up against the issue "head-on" with the desire that the students preparing for business or industry will be swift on the issue and will be comfortable through school coursework with the proposition of moving nearer and exploring the condition’’. (Forcht 1986)

As growth, creativity and technology fields have evolved, the extra time and imperative to examine security ideas have been accepted. In the late 1990s, Mayo and Kearn researched supplying students with a laboratory in which they were able to study programming and design concepts in a semi-committed state (Mayo & Kearns, 1999). The lab was structured to demonstrate, when a student attempted programming or operating devices, that the Transmissions Control Protocol / Internet Protocol should be used. While this situation was not produced specifically for advanced security guidance, it acts as an early example of how computerized security principles started to work through advanced safety guidance.

The country's IT specialists remain unknown due to the very few learning institutions that have such advanced programmes in South Africa (Van Niekerk, 2017). The probability that people, in general, will simply grasp the delicacy of IT systems and that students in undergraduate software engineering programmes need to be more aware of these problems (Yang, 2001). ISO-27002 has been published by the International Organisation for Standardization (ISO) on security mechanisms. These principles have contributed to an evolving trajectory in a universal and national information security arrangement. As a result, teachers are meeting the wishes

that public industries demand from information security experts (Van Vuuren, Phahlamohlaka, Leenen & Zaaiman, 2014).

South Africa's security career is focused on seller developments and technologies, i.e. database security is gradually being lined up with database merchants such as Oracle, whilst network security to vendors like Cisco and Huawei (Cisco,2017). This is not beneficial since the origins of cyberattacks is not fully known.

There is a need to develop new solutions to consider the holistic scholar and potential workers. According to Schleicher (2018), 26 OECD members stress the fact that they must understand the innovative ideas possible to address the problems of the changing planet. He regretted that environmental, cultural, economic, and technological developments have been so drastic that they need to notify all OECD countries (including South Africa) about their 2030 vision of education. He also warns that apart from our training system, the exponential growth of research and engineering will deepen the gap between countries and individuals of society and will compound the social divide.

Without a purposeful curriculum for cyber security in the interest of each country's sovereignty, institutions constantly depend on imported qualification programmes, which feed their authors' substances. For example, multi-nationals deliver cyber training programmes which are consistent with their expertise as mentioned below (Cisco, 2017):

- Cisco: Cyber security Experience Centre and Academy
- MICT-SETA: CISCO Funded Cyber Security Training Programme
- IBM Bluemix: Digital Privacy & Cyber Protection
- Oracle University: Oracle Security Certification

This has partially produced a safety professional that is not well rounded and responsive to the demanding and evolving environment at all security levels. In this strategy, the defence experts are less able to cope with cyber-attacks from any type of interconnected network element. Users must develop Cyber security experts with different capabilities and different settings.

As an OECD Member State, it should promote a wider education agenda and train our potential cyber workers to have an impact on their world and be able to meet future challenges. More generally, the defence should not only be a specialist area but a constant effort by any researcher to see protection as a fundamental building. In this way it is possible to consider a multi-faceted approach to security education that embeds us in the daily digital activities, making it particularly confidential, i.e., it can be called "cyber-literacy" in the South African sense if it is deeply founded.

Olson (2016) also advocates that defence curriculums should be mapped to business to ensure that a deficit in expertise is filled not by the few experts that are built by the narrow, self-serving services provided or funded by multinationals but by all those with defence literacy. Another critical risk faced by South African businesses is the outsourcing of Cyber security resources owing to a lack of data security expertise. Any state body, any agency, must maintain power and control while cyber matters are at stake, and this is not feasible to continue to have command and control by ill-considered outsourcing policy (Cloete, 2012).

Chandarman (2016) criticizes these outsourcing techniques as well since there are security risks that are underdeveloped by local talent. Cyber security analysis is still stunted and ignored as an important arena in developing new principles (Fourie, 2014). On this outsourcing tactic, organisations often appear to render outsourcing countries susceptible to cyber-cold war as their data control is already lost. Some prominent government institutions have also migrated (if not all) ICT systems into the cloud outside of South Africa (Cloete, 2012). SITA, in circular 10 of 2016, was asked to vet these clouds, although SITA is searching abroad for such clouds due to lack of local resources or human capital and to ensure that they are covered (Donovan 2015). It would be impossible to protect our currency from being exposed in this way without a well-trained cyber workforce.

It is important to develop skills not just because of national security interests but also to restore employment that has been outsourced to other companies outside South Africa. The cornerstone of our NDP Vision 2030 which coincides with Vision 2030 of the OECD Member States (Department for Telecommunications and Postal Services (DTPS) 2016) is job creation and innovation. As Morgan (2003) reports, they are headed towards a skills crunch in 2022 and beyond with an expected global shortage of around 31 million unfulfilled workers. The following styles of technical qualities are expected for potential workers (Kirlidog, Van der Vyver, Zeeman & Coetzee, 2016).

- Sensemaking (capacity to decide the more profound importance or centrality of what is being communicated)
- Social knowledge (capacity to interface with others profoundly and directly, to detect animated responses and wanted communications)
- Novel and versatile reasoning (capability at considering and concocting arrangements and reactions past that which is repetition or guideline-based)
- Cross-social skills (capacity to work in various social settings)
- Computational considerations (capacity to decipher tremendous measures of information into unique ideas and to comprehend information-based thinking)

- New media education (capacity to fundamentally evaluate and create content that utilizes new media frames, and to use media for enticing correspondence)
- Trans-disciplinary (education and capacity to comprehend ideas over numerous controls)
- Design mentality (capacity to speak to and create assignments and work forms for wanted results)

The professional attributes defined above came about because of certain six key drivers that call for these kinds of professional attributes. These key drivers as researched by Kirlidoget al., (2016) are:

- Extreme lifespan
- The rise of savvy machines and frameworks
- Computational world
- New media nature
- Superstructure associations
- Globally associated world

Cyber security is one of the leading sectors that has a more favourable connection with the market for these qualities compared with the experimental cyberlearning industry. When one knows that Cyber security curricula can be used to inspire a potential Cyber security specialist, South Africa can even gain from exports of expertise, creativity, etc.

If the country can improve skills, it must begin at the grassroots level, i.e. at primary, secondary and tertiary level, where there must be change of curriculum. The impact of the curriculum reform is a result of many factors according to the Bicak, Liu and Murphy (2015) model in their proposal report about the use of cyber security growth specialities. In the following Table 2.3, you can examine the need for a change in the curriculum in South Africa:

Factor	**Assessment of SA**	**Decision**
Diffusion of innovation theory	This means having the right expertise to explore and develop new curriculum	Develop the expertise. South Africa does not have matching expertise that can use new knowledge in developing an innovative curriculum

Current technology application status in the industry	Globally, the 5 leading countries on Cyber security innovation account for more than 75% of market share for an industry worth of $2 trillion.	Construct a labour force that can improve and innovate. Deprived of enough prepared digital workforce, South Africa won't develop and submerge the business utilization of digital improvements
The impetus for the new topic	Many curricular world-wide has been developed due to increasing interest, relevance, and demand for Cyber security	Aside from the Education Officials The digital force has not contacted our instruction authorities, and this must change.
Status of new technology adoption in other organizations	The emergence of threats from the cyber landscape has brought in new innovations that are being worldly adopted even though standards are a slight hindrance	South Africa is no exception, these new technologies need capable cyber workforce not only to operate them but innovate them further. Our cyber education curriculum is a key determinant of success
Technology certification status	Presently affirmations programmes are seller explicit essentially driving their plans for amplifying their primary concern	Seller one-sided arrangements won't progress NDP Vision 2030 The direction is required on our instructive system to provide guidance on the substance and expansive nature of our educational modules
Avoiding curriculum bloating	The educational programmes must be overhauled with the end goal that it doesn't convey a weight to researchers, instructors, and executives	Consider utilizing a multi-pronged methodology of augmenting current educational programmes or innovate and introduce new content to our current security challenges
Level of risk	The danger of not having a skilled state whereby its natives are not ready to take care of their issues may appear as if the instruction isn't being attended to	Structuring an instructive technique and an arrangement on any field that will be affected by innovative changes will diminish the danger of not having a competent state whenever overseen appropriately.

Table 2.3: Analysis of a strategic model for "when" decisions (Bicak, Liu, and Murphy, 2015)

One lesson for South Africa from Lui and Murphy (2012) is how to build an adaptive Cyber security curriculum that creates a skilled and adequate cyber workforce capable of developing and innovating cyber technology, for South Africa to realize its NDP Vision education goals 2030. Career pathways must open to fit the virtual world.

Powerhouses in cyber defense like the United States, the United Kingdom, China, Russia, and Israel have been successful in developing a career path from primary levels.

The UK Cabinet funded Cyber security initiative found that the system was not fast enough and hence the expertise differences in the cyber environment (Volz & Shepardson, 2017). To build this pipeline at an early stage, they must follow a structure that has supported the five-strong nations in the cyber domain. These countries have developed such a professional cyber workforce with a multi-level, multi-stage and multi-disciplinary approach (ML-MT-MD) (Sobiesk,et al., 2015)

She also says that teachers should obtain tools in the early stages to teach technology curricula not only as a separate topic but also integrate Cyber security into current curricula. In its very nature, Cyber security is part of our lives, and it should therefore be integrated into and extended into these top organisations.

This portion may be used to get the conclusion that South African higher education institutions don't do much to produce skilled data security professionals. It is crucial to investigate the lack of a framework for the development of cyber security education. It would be innovative to conceptualize a framework for the development of a curriculum for cyber security.

2.6. Course Development and Maintenance

In the last decade, a great deal of study has been carried out about how security ideas can be integrated into the education programme of data engineering and render them to be more sustainable. Some models have been suggested and the examination has been circulated to create a persuasive instructional module for information security.

Crowley (2003's) study of evidence confirmation and data validation education systems is notable in the implementation of curricula and instructional programmes. He researched the probability of the information affirmation, the future jobs of work candidates, advanced security planning accomplices and an attempt to establish a normal approach to data collection. His view was that security problems relied on the context in which they arise and that, from a

particular viewpoint, they were complex and innovative because of their flaws, their distribution, and the kinds of counter-measures necessary. He believed that information and data acknowledgement were based on too many criteria. It covers "brain studies, human science, law, programming creation, computer planning and the council" (Crowley, 2003).

This indicates that protection is a multidisciplinary environment of dominance from a wide variety of areas. The complex fragment recommended that "not in a few areas, seeing what to do and why it should not be based on an affiliation's identity assurance," the last item was that acknowledging how security concepts should be implemented was an odd bit of a protection instructive initiative. These considerations have been implied during the past decade more than once since they were dispersed.

Over the decades, diverse quantities of the debate have been debating how these factors can be related. For starters, Border and Holden (2003) perceive how to better combine security thoughts in the mid-2000s. During their inspection at Border and Holden, they spoke with the IT workers about how best to improve security training in IT educational programmes. They say that everybody thought the best way to connect securely. Some felt that additional courses were better incorporated, others trusted that protection express modules were better tailored for each purpose of the analysis. "Different researchers have transmitted the requirement for the security-over of the IT-instructive module. The suggestion to accentuate computerized security should not be treated as a counterfeit against this review and as a robust warning against extracting security contents from IT designates so that it is transferred into the ad-described object. Following a study of two or three cases of instructions, Rowe's and others' best approach to handling protection in education systems tends to be a model.

O'Leary's analysis acknowledged the nature of the Towson University security programme. The safety course of the capstone stressed: "guaranteed instruments and structures for the weakness of surprise attacks" (O'Leary, 2016). Students were split into classes and eventually worked on top organisations including controlled firewalls. A subsequent laboratory would then concentrate on observation. O'Leary found that students expected to customize their devices deliberately. When they didn't, diverse people easily dismissed them. O'Leary was inspired to investigate whether the instruction was satisfactory for students to understand and respond to state-of-the-art cyber-attacks that formed the basis for curriculum developments.

Otherwise, models are demonstrating how to best prepare and instruct the module. Van Vuuren et al., (2014) agreed with some elements of O'Leary. The goal of the course was, in their opinion, to allow students to take a similar opinion as a programmer and to appreciate the way

a software engineer thinks and appreciate the point of view of such experiments, their gadgets and their positive results (Van Vuuren et al., 2014). The hands-on laboratories were developed in compliance with the OWASP Top 10 Web Application and Safety Threats (Van Vuuren et al., 2014). The laboratories had a pre-changed contraction running a web server and sites with multiple vulnerabilities. According to Van Vuuren et al. (2014), the cornerstone for the course will be the Open Web Application Security Project (OWASP) Top 10.

This is one example of how practitioners strive to develop certain instructional modules to meet a market adjustment. Another model, which is not explicitly connected to computerized defence, demonstrates the consequences of constantly evolving knowledge on courses. Helps (2010:12) exhibited several imperatives, where educators viewed 'advance improvement as a crucial collaborator in improving their courses in many situations.' The second was that there were two templates developed for instructor approaches: the courageous achievement emerges, and the formal presentation.

The debate on the most optimal approach to the grasp of safety issues in education modules will continue to be explored by instructors and researchers, as fresh knowledge turns out to be structuring and incorporating data security into the courses. Leadership in digital security has made great strides.

The KBP Pedagogical Model, as illustrated hereunder in figure 2.3, (Endicott-Popowsky &P Lipovsky, 2014) is the ongoing progress of the KBP Pedagogical Model for the creation of information security experts, which gives an analysis of the structure of curriculum growth and provides inputs for capital (potential students), the labour market and developments of the broader social and economic context.

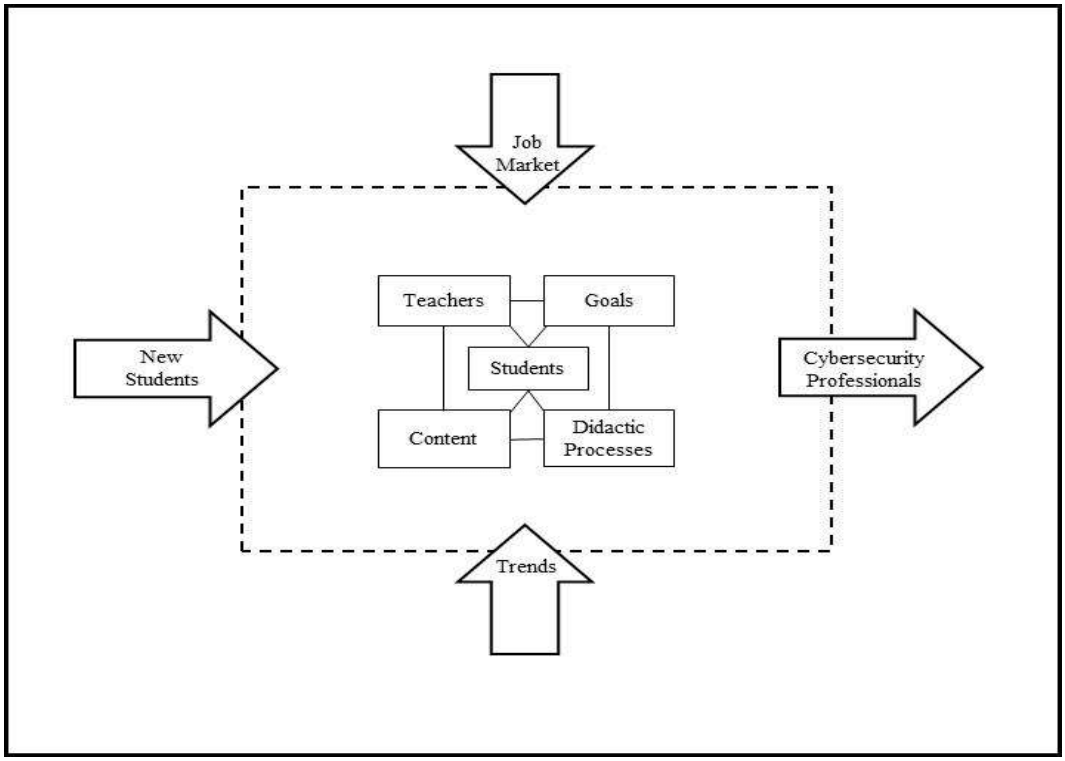

Figure 2.2: KBP Pedagogical Model, (Endicott-Popovsky & Popovsky, 2014)

These aspects form the curriculum collectively, the learning objectives of the programme, students, the curriculum material, and pedagogical processes. It highlights further factors of organisational design that supplement the KBP model. It explains how these elements are designed to fit together to integrate the technical and business concerns of veterans seeking future Cyber security leaders.

In addition, participation in training with hands-on learning continues to evolve. The fundamental engineering used to promote these ideas has gone from minimal physical environments to virtualized conditions that allow for more undergraduate studies. More introduction to web security is the development of more seasoned system security rehearsals and rivalries with digital barriers are a common additional source of learning and assessment.

2.7. Critical pre-requisites for Cyber security in IT

There is no denying that every information and technology program should ensure a rigorous and universal security curriculum in its courses. If it were not, students would not only be disadvantageous but also potentially risky for preparing students with specialized technological experience but without a sense of protection – such an absence would almost inevitably lead to applications that are developed or created by graduates with significant security vulnerabilities.

However, advanced Cyber security curricula are ideally suited for IT programs. The five pillars of the IT curriculum were earlier defined by Idziorek, Tannian, and Jacobson (2011) as being scripting, networking, human-computer interface, databases, and online systems. Each of these five pillars is a crucial requirement for cyber security. The following is a justification for this (Idziorek, at length, 2011):

i) Programming

The most fundamental skill taught in an IT curriculum and all computing programs is probably how to program a computer system to produce the desired result. However, this is where there is a chance of unintentionally creating vulnerabilities that can be exploited. Computing security breaches are frequently caused by programming security flaws. Even the most skilled programmers can make errors, and even a minor oversight can have significant consequences. Similarly, the capacity to address these weaknesses is found in programming. To comprehend how and why a software vulnerability could be exploited and to start understanding the consequences of a successful assault, conceptual programming expertise is at the very least a crucial cyber-security tool.

ii) Networking

Cyber-security requires understanding of practical networking. A networked collection of entities is referred to as "cyberspace". Advanced cyber-security education has several important prerequisites, including an understanding of computer network ideas, technical details, protocols, and vulnerabilities.

iii) Human-Computer Interaction (HCI)

HCI is a significant "piece of the pie" in the context of cyber security. User mistake appears to be the main reason for security breaches, despite reports to the contrary (Idziorek, at el., 2011). Is this the result of inadequate user interface design or inadequate user training? Both are probably going to be important. Information technology specialists are referred to as user advocates and successfully act as a human interface between users and technology. They oversee ensuring that users may achieve their objectives through the right use of computer technology in an efficient, secure, and effective manner.

User advocacy heavily relies on user education. Users can learn to identify and stay away from typical security problems including phishing attempts, social engineering, malware, and unsafe surfing through effective training. These strategies have already proven to be beneficial, and as of 2009, user mistake is no longer the main reason for security breaches.

iv) Databases

In cyberattacks, databases are frequently the main targets. They are a valuable source of knowledge that frequently contains sensitive user data, commercially sensitive information, or both. Information Technology provides a substantial amount of information on database management systems (DBMS) and database administration (DBAdmin), but other computing programs could place more of an emphasis on sophisticated database structure and design techniques. Although these are meant to improve students' theoretical and practical system integration and management abilities, an understanding of database management system operation and administration are crucial skills in protecting information from cyber-theft or sabotage.

v) Web Systems

Many kinds of computer systems have an external access provided by web systems. The first publicly available boundary that an attacker will communicate with in cyberspace is often a website. Websites serve several functions and are frequently a good attack vector for a company's internal network. XSS, or cross-site scripting, is a particularly pervasive and dangerous problem. This is a type of drive-by infection, where malicious code is injected into a victim's device without their knowledge or consent using vulnerabilities on the customer side. XSS places malicious code on an attacker-controlled website that uses the vulnerabilities to insert customer side coding into a legitimate and typically fast website. The likelihood of this type of spread depends on the malicious code's design, which can range from privacy invasions and identity theft to complete remote control of an attacker's target system.

Websites are intentionally located in a public space, so great care must be taken to protect them. Additionally, security researchers find problems and report them to companies, who then upgrade their products or release security hotfixes (Kessler & Ramsay, 2014). Every web presence company should have clearly defined regulations for manufacturers' solutions because

this developmental twist seems to have no end. The foundation of web-based IT systems includes a strong security focus that handles additional security concerns such the requirement for server hardening, firewalls, and IDS/IPS.

As seen, the five foundations of IT are suitable for education in Cyber security (Idziorek, at el., 2011). A robust security aspect already exists across each pillar, which offers students subject-related information that is both intellectual and technical in a security sense. These same foundations also include crucial information that is important for cyber-security education.

Components of the cyber security curriculum are found in different professions (Jontz, 2015). This richness must, in fact, be encouraged and used as much as possible for interdisciplinary collaboration. The distinctiveness of computer science, computer engineering, electronic engineering, information system organizations, and many other professions that share an interest in cyber safety will be preserved thanks in part to our digital society.

Kessler and Ramsay (2014) concur that IT offers the best environment for cyber security education, setting it apart from other disciplines. In fact, if a brand-new concentration were to be created specifically for cyber security, it would resemble an information management curriculum with an emphasis on cyber defense.

2.8. A Cyber-Security Curriculum in educational curriculum

In various ways, we have addressed some concepts of cyber protection and the suitability of IT programmes for this subject. This segment now addresses the suggestion for an innovative Cyber security education program. From the Section, the study demonstrates that even between the divergent views and meanings of Cyber security, a formal curriculum can be developed, which should cover these concepts as well as be impartial.

In several studies on security education in computing programs, the Center for Education and Research in Information Assurance and Security (CERIAS, 2018) at Purdue University proposes a layered approach to IAS education as (1) Prerequisite Knowledge, (2) Information Assurance Body of Knowledge, (3) Higher-Order Skills, and (4) Job/Professional Level.

Academics such as McGettrick (2013), Manson and Pike (2014), Manson, Curl, and Carlin (2012) recommend that the advanced Cyber security program is put in a higher range at the third level and introduces students to level 7, wherever possible, as mentioned in this section:

i. Outcomes

To build a successful programme, it is important to set goals and outcomes. Such aims should be curriculum specific and customized to the teaching institution's instructional and research priorities. With this in mind, we will address five high-level findings, which can be generalized to most systems in a generic fashion. Students will learn about cyber security's multidisciplinary and quick-run existence and will learn and appreciate emerging innovations and perspectives throughout their careers. This result is based on a study carried out by Crowley (2018) which explores the creation of the curriculum in information security. It is stated how the IAS is multidisciplinary, encompassing psychology, economics, law, information technology, engineering, and management. They should also have a crucial mathematical, physical, and IT feature in cyber defense.

In the realm of cyber protection, they should also have an important mathematical, physical and IT feature. Students learn fundamental skills in data security with a concentration on a career journey. This conclusion was taken from Eugene Stafford's NCISSE presentation at Purdue University in 1998. It emphasizes the significance of aligning a curriculum with a career. Students can talk about the topic with a variety of professional and non-technical audiences and are aware of the necessity for inter-disciplinary and inter-cultural data security collaboration.

As seen from the Brigham Young University IT objectives (2019), Cyber-security emphasizes results. Students need to be able to transcend cultural and academic boundaries to enhance device stability and inform consumers. In the area of Cyber security risks, assaults, accidents, and protections, students may be able to extend their system integration information laterally or 'outside the box.'

Another consequence of BYU's IT curriculum is the need for data security experts to step outside of the box to "link the dots." Being able to think of a cyber victim as a possible intruder, and knowing the broader picture, is critical in Cyber security. In an advanced, persistent threat scenario, for example, a network security specialist should be able to identify and correlate all attack vectors using a root-cause analysis to define attack targets, begin building on the attribution, and execute an incident response strategy that minimizes service interruptions and improves defenses.

A brief video (of unknown origin) depicting two government representatives pleading for help after an escalator breakdown is one of the regular components of BYU's Information and

Security Class presentation. The anecdotal example serves as a stark reminder of how easily daily routine may veil our thinking and how important it is to be aware of this.

The students will be aware of the ethical requirements of the computer security industry and will treat financial, moral, and privacy considerations with respect and consideration. As a final consequence of our focus, we emphasize the importance of high moral expectations for Cyber security practitioners. Other scholars also stress the importance of spiritual and ethical education in safety-related matters (Rowe, Lunt, & Ekstrom, 2011).

These five conclusions shouldn't be viewed as exhaustive. They are only provided as a support for those in charge of course design and as a starting point for creating content for cyber security programs.

ii. Security Across the Curriculum

According to several academics, IT security curricula are crucial (Rursch, Luse, & Jacobson, 2010). The recommendation to put more of an emphasis on cyber security should not be seen as contradicting this research, and we strongly caution against moving protection information from IT organizations to specific cyber security training sessions. Their implementation has demonstrated the benefits of protection in the curriculum (Rursch et al., 2010). Rowe et al. (2011) however, assume that there is already considerable advanced material that can support graduates and reduce the technical Cyber security gap.

Some scholars say that security organisations are taken from several scholarly fields rather than from a separate analysis (Smith, Koohang Behling, 2010). Although Cyber security currently unites different academic disciplines, it does not mean internal cohesiveness or creative content. Currently, as we show, certain subjects aren't found in any other discipline. We assume that this is partially a factor in the current shortage of trained practitioners.

The Committee on National Security Systems created an educational reference framework in 1994 that includes protection content from many different disciplines and lists the information security curriculum awareness-body (Thaw, 2014). The NSTISSI 4011 material sections cover the principles of communications, security, NSTISS, operating system setting, preparation, and management, as well as NSTISS policies and procedures. Although this provides a solid basis for security and information management education, it does not address any current cyber issues. We encourage organizations providing information technology or comparable organizations to consider including an advanced cyber safety curriculum (NSTISSI) 4011

considering the IT model curricula and the National Preparation Standard for ISS Infosec (NSTISSI) 4011 (Zepf, 2013).

iii. Organisations

Ekstrom and Lunt (2018) presented a study in 2003 before the IT Model Program was developed, that attempted to define IT as an academic discipline rather than a broad view of the current disciplines. Their analysis described a crucial field, "machine integration," which the computer programmes did not cover. Systems convergence eloquently defines one of the main priority fields of IT (Smith, Koohang Behling, 2010).

In recent years, IT has evolved to cover in detail how numerous technologies can be implemented to allow users to improve their cyber security apparatus. This emphasis has been refined but there is still potential for improvement as the program is refined (Ekstrom & Lunt, 2018). The IT discipline is very much alive by its existence and ties with several socio-tech areas, including social computing, technology education, scientific innovation, and Cyber security.

Given the improvements in cyber-security requirements, reports, and documents, it would be wise to prevent further confusion at this point. In our experience, it is a good method to motivate students to examine these discrepancies. According to Schnieder (2013), "plurality cannot be without need," but conclude that simplifying cyber protection in a few keywords and relationships would offer a scalable structure. This versatility encourages programmes to retain a comparatively 'open' academic system that can adapt to 'sand moving' problems in concepts of Cyber security, requirements, and frameworks (Schnieder, 2013). The research suggests that an advanced perspective on data protection should be found in three high-level categories pursuing a standard precondition for information security. The following categories are planning, protection and regulation.

Initially, the inclination was to categorize the latter as a "reaction" to a cyber-incident. In light of the principle "It is better to act than to respond," this looked inappropriate. In contrast to a well-thought-out action plan, the word "respond" can conjure up notions of a careless reaction to the knee. The following inquiries can help to better contextualize each of these groups:

- What cyberthreats exist, and how can systems defend against them and prepare for them? (Preparing)
- How do you create and keep up secure systems? (Defending)

- What actions should be taken in the case of a cyberattack, and how can one assign blame? (Acting).

Cybersecurity preparation makes ensuring that the dangers are recognized. This necessitates a thorough comprehension of the threat and its ramifications. It's critical to keep in mind that it's not only technical. Planning must consider how internet and the physical world interact. The main scientific topics include advanced persistent/evasive attacks (APT / AETs), ethical hacking, and penetration testing.

Cyber security involves the protection of information networks which involves both technological which non-technical aspects once again. The assumption is that this category is appropriate for device management. Systems Administrators are responsible for managing and enforcing compliance protocols for systems and networks. Additional related issues include the architecture of networks and applications in a security context. The preventative defence area covers hardening, audits, accreditation, and consumer education.

The type of behaviour is what to do in case of a cyber threat. What are the symptoms of an active attack? How will the possible consequences, attribution, response and return of operation be assessed? Digital forensic organisations (live and offline) and reaction to accidents are technical subjects. Additional fields include global and cultural standardization, regulatory concerns, counter-forensics, philosophy of electronic forensic investigations, and incident management and understanding the diverse methodologies and goals of various organisations.

For each group, recommended courses include cyber-threats and intrusion testing, cyber-defence and system management, and cyber-response and forensic investigations.

It should be remembered that each issue is connected to a more professional activity. This pairing purposely involves classes that discuss both the principles of cyber-security and a realistic toolbox for a cyber-security professional. This relatively high degree of subject abstraction should allow lecturers to concentrate on a particular cyber safety model, if desired, with considerable versatility in content and academic freedom. At the same time, it stresses that cyber defence is not a new issue, but rather a way of seeing and correlating current information that analyzes, acknowledges, protects, and responds holistically to cyberthreats. (The OECD report 'Reducing Systemic Cyber-Security Threats' offers an outstanding mid-level overview of cyber-security issues and points of debate).

iv. Educational Methods

Excellent information on teaching strategies for security organizations has been supplied by several researchers (Ekstrom & Lunt, 2018). Reviewing the current supplemental instructional approaches that have been proven beneficial in our program is necessary in the hopes that they will help course designers. This list can be used as a starting point for more research even if it is by no means comprehensive.

v. Hands-On Exposure

According to the study (Schnieder 2013), practical experience is a crucial teaching tool. The idea that "hands-on learning is at the core of science education" is widely held, but Nancy (2019) emphasizes that laboratories should be deliberately directed toward conceptual education. Several laboratory teaching methods were examined in 2006 by Jing Ma and Nickerson, who concluded that labs can be a crucial tool for both philosophical and design preparation.

There is no question that a well-designed laboratory will be very useful in learning to students. Experience has demonstrated that students benefit from laboratories that facilitate critical reasoning and other higher cognitive functions. Cyber security is an especially suitable subject for laboratory training since many laboratories are unscripted and 'open-ended,' such that several right solutions are feasible. Allowing students to choose instruments, technique structures and operating systems to accomplish an aim and promotes study and creativity under the guidance of students.

According to Dittrich (2017), students with a focus on cyber safety can be compared to military training regimes, which address the importance of expertise and problems with fast-dating technology. Care must be taken in the construction of cyber-security laboratories to ensure that the practice is not solely associated with devices or applications, but relies on principles, methodologies and expertise that can survive the time test.

One popular strategy is Cyber security simulations or cyberwar games. Students are placed in a competitive environment as a result, which motivates them to grow as individuals and accomplish a goal. Such activities are popular with hacker groups and agencies. White (2018) identifies an activity college that eventually takes place at the national level.

vi. Collaboration

In a teaching environment, students can get a valuable perspective into emerging Cyber security challenges, developments and demands by collaborating with industry and the government. Encouragement of cyber-security experts to apply for positions or more well-organized programs to expose students to real-world settings should both be considered as collaborative opportunities. It's not necessary for such collaboration to be external, as one organization has demonstrated.

After an effective malicious breach of its data network, Dartmouth College has developed an effort to enhance protection by students in coordination with the campus computer services (Martin, & Choo, 2014).

Several scholars have acknowledged the need for data security knowledge sharing (Mandiant,2015). By proper cooperation, students would understand the need for (and play a role) exchange of knowledge between the society, the private sector, and the government. The most recent Cyberspace Strategy Analysis confirmed the necessity for this kind of collaboration by demonstrating the need for a variety of combined efforts involving the public and corporate sectors as well as academia (Kessler & Ramsay 2013). Collaborative activities give students the chance to become acquainted with the educational process and motivate future professionals to earn credentials (Gemalto, 2015).

2.9. The Cyber security body of knowledge

Cyber security information CyBOK is a unique platform that offers an invaluable knowledge base for the first time, covering the scope and depth of Cyber security, which shows that cyber safety includes a wide spectrum of disciplines (Viveros, 2013). A framework for the development of the cyber security profession was established with the launch of the Cyber Security Body of Knowledge initiative in 2017. The project's primary goal is to formalize the profession's foundational understanding of cyber security. The project also allows the formation and career paths, curricula, and vocational training to be established. The Version 1.0 of the CyBOK was published on 31 October 2019, formally launched in January 2020 and the next phase of the project (until March 2021) will focus on the dissemination and application of CyBOK (Mandiant, 2015).

According to Gemalto (2015), CyBOK covers both physical and virtual security of data, software, and hardware against damage from allowed and unauthorized access, whether the

access is internal or external. Technology is used to carry out preset procedures for cyber security. Since technology is developing quickly, it is not only difficult but also essential to plan out the security process; as a result, practitioners share their best practices and lessons learned (Dittrich, 2017). Protecting the server room, where it is located, the switches, the cable, the data and data storage devices from fire and intruders using high heat are only a few examples of what is meant by the physical security of data software and hardware from allowed and unauthorized access.

As a result, server rooms are frequently air-conditioned, fire-insulated, and have floors that are raised to dock the cables (Zepf, 2013). In addition, wires are docketed in walls or beneath a raised floor, and switches are typically located in high, hidden locations to limit reachability. Another issue that falls under the category of physical security is the location of the server room. The ensuing matrix (Conti, Babbitt & Nelson, 2011) summarizes the key topics that are relevant to this topic.

Another layer of security should be in place for authorized personnel to access the IT systems, ranging from password-protected access setup to magnetic card to retina scan to lock and key, as shown in Figure 2.4 below. Physical security and non-physical security, though, are frequently not limited to dangers from the outside and may even be taken into account inside, depending on whether the assessed damage is regarded purposeful or unintentional. However, non-deliberate damage is reduced by appropriate instruction and training, whereas purposeful damage requires the establishment of strict policies to assure staff compliance and disciplines such cameras and employee follow-up (Conti, et al., 2011).

	Physical	Non-physical
Data	Keep copies in different locations	Ciphering, password
Software		
• Operating system	Copies	Password/biometrics
• Application	Copies	Password/biometrics
Hardware		
• Network	Not visible	Password/biometrics
• Server	Location/fire distinguisher/air condition	Password/biometrics
• Switch	Location	Password/biometrics
• Cable	Embed in walls	Away from power

Table 2.3 (Conti, et al., 2011) Interactive computer system threat matrix with physical and non-physical dangers.

Figure 2.5 below shows the interaction of physical/non-physical threats with the conductor of the threat internal and external.

	Physical	Non-physical
Internal	Damage to hardware & software (intentional or non-intentional) set policy and provide proper training	Viruses: limit access to external systems +policy
External	Physical attacks	Hacking +viruses: Fire walls + antivirus

Table 2.4 The Matrix. (Conti, et al., 2011).

Given that the system is more significantly threatened by unauthorized use and access than by physical damage, the non-physical harm is not only more sensitive but also extremely hard to monitor. Since viruses pose a serious risk in this scenario, access to the system should be strictly regulated through the employment of rigorous policies and effective antivirus software. Although software tools like firewall and antivirus may protect the system, as shown in Figure 2.5 above, the external threat of damage like hacking and viruses poses as the most difficult. On the other hand, the external physical threat, like attacking and robbing ATMs or physically attacking a server room, switches, cables, and data, can be defeated by putting in place concrete measures. These techniques can include, but are not limited to, installing servers in secure spaces, making sure that switches and cables are hidden from view, keeping data in secure locations with backup copies, and utilizing massive storage.

The core elements in Cyber security are the following 12 elements; these are the pillars or the base to any Cyber security programme:

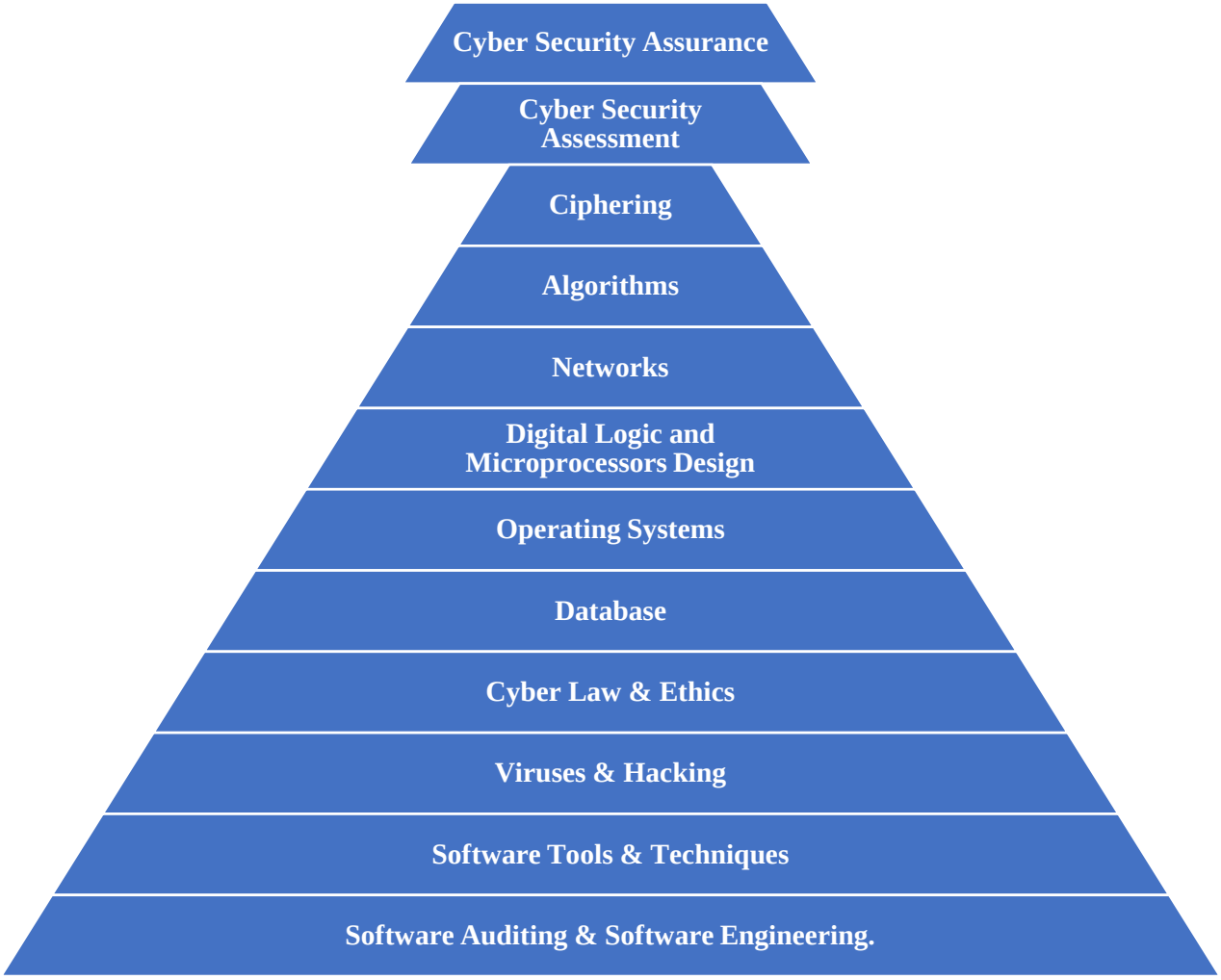

Figure 2.4 The core elements in a cyber security program, (CyBOK, 2011).

The 12 pillars and essential components of the body of knowledge for cyber security are further explained in the sections that follow.

i. Cyber security assurance

Lipner (2018) offers the clearest definition of cyber security assurance, along with instructions on how to attain it. According to Lipner's definition of assurance, "assurance: making systems that can resist attack." He continued, saying that "Assurance is achieved by integrating security into the process of designing, building, and testing systems" (Lipner 2018: 12). Himchak (2015) did study in this regard. The authors offered a thorough curriculum with a focus on software assurance to build a software assurance curriculum for master level and again to develop a software assurance curriculum for master's level. An approach like Mission Risk Diagnostic (MRD), which is used to evaluate risk in systems across the supply chain and life cycle, must be learned by cyber security specialists, according to Himchak (2015). A expert also has to understand SQUARE. SQUARE is a nine-step method that enables businesses to include security, including privacy, into the very beginning of the product lifecycle.

ii. Cyber security assessment

According to Idziorek, Tannian, and Jacobson (2011), an assessment framework was developed and was adopted by 30% of organizations, and it consists of two parts: Inherent Risk Profile and Cyber security Maturity. The assessments are conducted in domains according to five levels of maturity according to the FFIEC (2018) suggested model. Additionally, the cyber security professional should be able to design and carry out a cyber security assessment by comprehending the various methodologies used across all industries to manage a cyber security assessment, conduct a risk analysis, and counteract various cyber security threats. first, comprehend cyber threat attack analysis reports and write them. Second, comprehend assessments and create a cyber security policy based on them. Third, look for and examine instances of threats and attacks in action. Establish cyber security measures based on recognized models and frameworks as the fourth step. Manage the attack defenses as the fifth step. Sixth, reduce the dangers of threats and assaults. Seventh, after such assessments have been completed, a cycle of reports and evidentiary procedures for prosecution.

iii. Ciphering

Data can be transported safely and securely from one location to another via ciphering, which prevents anyone from viewing the data being transferred. Despite being an old method, ciphering is still necessary for security. In addition to ciphering algorithms, there are several types of ciphering that involve hardware, software, tools, and strategies.

According to the sort of operations carried out (substitution, transposition, bit manipulation), the cipher process (block or stream cipher), and the key, ciphering algorithms can be categorized as symmetrical and asymmetrical. Therefore, for a cyber security specialist, block cipher algorithms like IDEA, RC2, RC5, CAST, ElGamel, DSA, and Skipjack are crucial. In-depth coverage should be given to subjects including cryptanalysis, hash functions, digital signatures, and web security (CyBOK, 2011).

iv. Algorithms

Software is built on algorithms (CyBOK, 2011). Understanding the reasoning behind the software's fundamental components is necessary for software development. Data handling algorithms consider speed, storage capacity, and complexity. Data structures, compression, sorting, and search are all based on algorithms. To turn their ideas into functional software,

programmers, analysts, and designers communicate with computers using algorithms. Therefore, developing a security specialist's logical sense is a necessary quality. Sort and search algorithms, graph algorithms (such as graph traversal (DFS, BFS) and applications, strong connectivity, bi-connectivity, minimum spanning tree, shortest path, matchings, and network flow), and challenging problems (such as the traveling salesman problem, longest path, Hamilton cycle, Boolean circuit satisfiability, Clique, and Vertex cover) must all be covered in the typical course syllabus. Divide-and-conquer, graph traversal, greedy, dynamic programming, reductions, and the use of sophisticated data structures must all be included in the design of algorithms. The correctness of an algorithm must also consider tree and graph properties, as well as proofs and proof techniques (assumptions, fundamental logic inference and induction). Time and space complexity must be considered in algorithm analysis, and big Oh, small oh, theta, worst-case and average-case analysis, as well as lower bounds, must be considered in asymptotic analysis. Tractable and intractable issues require the use of polynomial-time, NP, NP-hardness, and NP-complete methods, NP Reductions.

v. Networks

The foundation of data transfer is networks, which are like the highways for automobiles. Anyone engaged in cyber security must be familiar with network types and standards (CyBOK, 2011). Networks include standards, a routing algorithm, hubs, switches, cables, and plugs in addition to devices like hardware. Additionally, the transmission control protocol and Internet protocol (TCP/IP), Open Systems Interconnection (OSI), and other computer network security models that adhere to the ISO standard. A network course often includes the following subjects: Link Layer, Media Access, Internetworking, Routing, Transport Layer, and Application Layer are the foundational layers. The Link Layer Services include Framing, Error Detection, and Flow Control. The Fundamentals & Link Layer comprises Building a network, Layering and protocols, Internet Architecture, Network software, and Performance. The Media Access & Internetworking comprises basic internetworking (IP, CIDR, ARP, DHCP, and ICMP), Bluetooth, Wireless LANs 802.11, Ethernet (802.3), and Media Access Control. The routing issue comprises multicast addresses, multicast routing (DVMRP, PIM), routing (RIP, OSPF), switch basis, and global internet (areas, BGP, IPv6). The topic of the transport layer covers an overview, UDP, reliable byte stream (TCP), connection management, flow control, retransmission, TCP congestion control, congestion avoidance (DECbit, RED), QoS, and application requirements. The application layer contains conventional applications like as HTTP, Web Services, DNS, and SNMP, as well as electronic mail (SMTP, POP3, IMAP, and MIME).

vi. Digital logic and microprocessors design

Microprocessor design and digital logic are essential for cyber security. This topic covers things like the structure and electronic architecture of contemporary processors, the principles of programmable logic devices, combinational and sequential circuits, and the principles of hardware design. Additionally, binary world, flip-flops, and logic gates are included.

vii. Operating systems

The layer of software that sits between hardware and applications is called the operating system (OS). Through OS, one can use a programming language to communicate with the computer hardware. Processes and threads, mutual exclusion, CPU scheduling, deadlock, memory management, file systems, and distributed systems are key concepts in this area.

viii. Database

In a computer system, data are stored in a database, which includes (but is not limited to) data models like Entity Relations (ER) and relational; query languages like relational algebra and Structure Query Language (SQL); implementation techniques of database management systems like index structures, concurrency control, recovery, and query processing; management of semi-structured and complex data; distributed and SQL databases.

ix. Cyberlaw and ethic organisations

Understanding the differences between cyber laws and regulations for cyber security is similar to understanding the rules and laws that apply to police officers. Knowing the laws and regulations governing the internet is crucial because there are no boundaries there. In addition to the authority that comes with such territory, there are also numerous ethical considerations that are relevant to the topic.

x. Viruses, worms, and hacking

Cyber security experts need to be familiar with the tactics, tools, and methods used to defend against malware software, viruses, and other threats. A police officer must be knowledgeable about criminal activities and their methods in order to do his job well.

To combat such issues, cyber security must be knowledgeable about the various varieties of viruses, worms, and hacking techniques. Malware includes everything from obnoxious malicious software to destructive cyberweapons. Furthermore, such software's detection, analysis, control, and elimination are crucial components of cyber security education. Tools like Dependency Walker, Fakenet, FileAlyzer 2.0, HxD, IDA Free, ImpREC, LordPE, Malcode Analyst Pack, OllyDbg, PEiD, PEview, Jsunpack-n. Internet Explorer Developer Toolbar, organisation script Honeyd, NetCat, Wireshark, curl, Off is, Radare, FileInsight, malfi apihooks, SWF Tools, Flare, and shellcode2exe are essential for Cyber security experts (CyBOK, 2011).

xi. Software tools and techniques

Software tools and procedures that are specifically designed for cyber security abound (CyBOK, 2011). The simplest are programs for managing databases, operating systems, networks, and other networks, as well as antivirus software. Consequently, experts in cyber security need to be familiar with these tools and procedures.

xii. Software auditing and software engineering

The 12th pillar, which is crucial to cyber security, is software audits and engineering. The majority of cyber attacks involve viruses or hackers that exploit a software vulnerability and can come from either internal or external sources. For instance, a programmer might have overlooked a port or a particular case. The appropriate steps should be taken in software engineering to prevent such a situation. Such an issue will be prevented by routine software and data auditing as well as the incorporation of self-tests within the software. Therefore, experts in cyber security need to be familiar with software engineering and auditing tools, techniques, and procedures. Security experts should be familiar with Software Assurance as well.

The Software Assurance Framework (SAF) is a group of cyber security best practices that programs can use across the supply chain and acquisition lifecycle. Therefore, cyber security experts need to be familiar with software security frameworks like IMAF. The CyBOK-recommended IMAF framework synchronizes drivers with recommended best practices for software security. Building Security in Maturity Model (BSIMM), Open Web Application Security Project (OWASP), Software Assurance Maturity Model (SAMM), Department of Homeland Security Measurement work and Assurance for CMMI Process Reference Model, and CERT Resilience Management Model are just a few of the codes of conduct that are listed.

Although non-core competencies and components are crucial, as technology is constantly evolving, additional courses can be established through self- or course-directed learning. Penetration testing, intelligence & counterintelligence, intrusion detection (analysis and response), and electronic evidence analysis are a few examples of such components.

An overview of cyber-security and the present problems in a framework of academic instruction are covered in this thesis. It is widely acknowledged that integrating cyber-security education and training into computing and other related programs is an effective way to raise students' awareness of the issue. However, it is obvious that the typical IT curriculum does not cover all of the facets of cyber-security. Institutions should have faith that the IT program creates a perfect platform for a foundational emphasis on advanced cyber security that goes beyond the already prevalent elements. Encourage IT professors to thoroughly examine the security of their programs' material to broaden their coverage of this crucial subject in acknowledgment of the model curriculum pillars of IT education.

As an emphasis on IT, a high-level framework for the instruction of cyber-security has been proposed. 'Prepare, Defend, Act' is the definition of the framework's three components. The challenge now encountered due to significant variations in standards, terminology, and procedures related to cyber-security is understood and acknowledged. The 'Prepare, Defend, Act' paradigm gives institutions the freedom to adopt a particular strategy or conduct an unbiased analysis of these variations. Within our own IT program, this framework is currently being presented as three graduate courses at the 500 level that are also offered as undergraduate electives.

Institutions have also provided strategies that have helped us strengthen our attention on cyber-security inside the IT Program, and we hope that this will serve as a springboard for additional research on successful strategies. It is to thank and respect the efforts of the government, numerous commercial sector organizations, academia, and open-source research groups in their

efforts to create a crucial awareness of cyber-security in reaction to the recent events that have transpired during the production of this study.

2.10. Information Security Educational Ontologies

The development of the Internet has many benefits for humanity. For the first time in history, people may easily connect and work together in almost real-time, regardless of international boundaries and/or time zones. Information technology has recently assimilated so completely into contemporary business that some authors no longer consider its use to be advantageous from a strategic standpoint. As an alternative, it might be claimed that information technology is a fundamental good, much like electricity, and that its absence makes it difficult to conduct business (Jacobson & Rursch, 2008).

However, the benefits of information technology and the Internet do not only apply to organisations. Increasingly, the Internet is being used as a tool for personal business, entertainment, communication, and many other activities by individuals at home. Online activities are also not restricted to only the rich, the educated, or any other specific demographical grouping. According to the World Bank (2010), 8.6% of all South Africans were Internet users in 2008. Amongst urban South Africans, this figure is substantially higher. Kreutzer (2017) found that 83% of low-income black South African youth in an urban township uses the Internet via mobile phone technology on a typical day. Even amongst school children, the use of online technologies and/or platforms has become almost ubiquitous due to the low cost of access using platforms like, e.g., MXit, WhatsApp. It can be argued that the Internet, in one form or other, today is being used by all demographic groups, including the young and old, rich and poor, educated and uneducated, urban and rural.

Unfortunately, the Internet has not only brought advantages. It has also brought numerous new risks. In an organisational context, typically these risks can be mitigated through the use of various information security controls. For organisations, these controls are usually selected with the aid of internationally accepted standards such as ISO/IEC 27002 and ISO/IECTR 13335-1. These information security controls largely depends on the actions of organisational users to work correctly. Humans, at various levels in the organisation, play a vital role in the processes that secure organisational information resources. Many of the problems experienced in information security can be directly contributed to the humans involved in the process. Employees, either intentionally or through negligence, often due to a lack of knowledge, can be seen as the greatest threat to information security (Kreutzer, 2017)

Organisations typically address this lack of information security-related knowledge through formal information security awareness and educational programmes. Many current research publications focus on organisational information security education and many companies specialize in providing such education as a service. Unfortunately, almost no one currently provides equivalent information security education for individuals using the Internet in their capacities.

The need for information security education outside the corporate environment has become widely recognized. Furnell (2018) likens the Internet to a jungle, with uneducated users falling" prey" to online" predators". Siponen (2019) identifies the need for five" dimensions" of information security awareness education, one of which is the" general public" dimension. Siponen (2016) also argues that society has an ethical responsibility to ensure that its vulnerable groups receive appropriate information security education. As an example; South Africans, in general, have a well-developed culture of personal security. Most South Africans are used to assessing the risks posed by "normal" day-to-day activities and know how to mitigate such risks, e.g., through locking the doors at night, avoiding walking through dark alleys, not leaving personal possessions unattended, etc. However, due to the relative newness of Internet access for many citizens, a culture of cyber-security is still lacking.

Many South Africans, especially from vulnerable groups, such as the elderly, are completely unaware of even the existence of many risks during "normal" online activities and thus can easily fall prey to online "predators". During 2010 alone approximately 4400 cases of identity theft, involving losses of more than R200 million, have been reported to the SAFPS (www.safps.org.za). As the so-called "digital divide" is reduced, progressively more South Africans will be put at risk of having their identities stolen. The only way to effectively mitigate this, and other risks posed by Internet access is through increased awareness of the risks posed by this medium, and education regarding how these risks can be mitigated.

There is a need for information security education for all "cyber-citizens". Furthermore, due to the diverse backgrounds, educational levels, and many other factors of the various vulnerable groups, a "one size fits all" approach to such education cannot work. It can thus be argued that an information security educational programme would have to be tailored to the specific needs of each target user group for such a programme to be effective. This study aims to argue that there is a need for a freely accessible "cyber-security portal" through which any Web user can access relevant information security educational programme. Furthermore, the study briefly explores the idea of basing such a portal on a Web 2.0, and hence E-learning 2.0, paradigm and then presents a call for further research towards such educational approaches.

2.10.1. Ontological approach to knowledge representation

For the purposes of this study, an ontology is a technology that enables the exchange of semantic data between individuals and technological systems. It comprises of a common domain vocabulary that has been encoded as well as a definition of each word's meaning. An ontology, according to Grüber (2016), is "a formal, explicit specification of a shared conceptualization." A machine-readable domain model that represents entities and their inter-entity connections is specified by a formal ontology. Typically, it comprises of a descriptive section and reasoning tools. The descriptive portion of an ontology expresses domain information in a fashion that can be processed by computers and understood by humans, capturing the domain from the perspective of the domain experts. With the aid of reasoning the data offered in an ontology can be used to learn new things.

A logic-based language called an ontology language is used to express the information in an ontology, which is then gradually developed. The availability of ontology languages with well-defined semantic organizations and potent reasoning capabilities is crucial for the creation and upkeep of ontologies. Thankfully, a type of organizations known as description logic organizations (DLs) already exists and allows for both, making them the perfect candidates for ontology languages (Grüber, 2016). The official Semantic Web Ontology language is Web Ontology Language (OWL) 2.0, which was given the status of a W3C recommendation in 2009.

Instead of only displaying web content, OWL was created to offer a standard method for processing it. It is not meant to be read by humans; rather, computer programs are meant to interpret it. In this study, the ontological model created for the strategic area of cyber security was interpreted using OWL.

Ontologies are the core technology powering the Semantic Web endeavor, and their use is expanding quickly across a range of application domains (NICE, 2017). Ontologies differ significantly in terms of their purpose and content (Singh, O'Donoghue, & Worton, 2005). For example, core ontologies only contain terms that are domain-neutral, meaning they apply to various sub-domains; upper-level ontologies describe generic, descriptive, and domain-independent terms; and domain ontologies reflect specific terms in a given domain and are detailed.

Ontologies are typically built with a specific objective in mind. Thus, an ontology's goals can be translated into a set of competency questions that specify the kinds of knowledge the

ontology should have (Gruninger & Fox, 1994). Knowledge management, information retrieval, portal and web communities, and e-commerce are four categories into which ontology-based applications can be placed (OntoWeb, 2002). These classes each have various specifications. The published materials and the three stakeholders—academics, students, and industry—will be used to compile the metadata for this ontological picture of IT-related organizations, subjects, and courses.

Model curricula like IS 2002 (Gorgone et al., 2003) and MSIS 2006 (Gorgone et al., 2006) are helpful specifications but they are also quite static, with modifications occurring as a result of re-evaluations that may take years to complete. Additionally, in addition to curriculum-related information, the knowledge base should also include information on other factors.

For IS education, a computer-based, Internet-enabled knowledge base holds the potential to be a more adaptable and reliable method. A effort to create an ontology for fields connected to computing and information was started in 2002 with financing from a number of accreditation organizations, including ACM and IEEE (Cassel et al., 2005; Davies, Cassel, & Topi, 2006). According to Cassel et al. (2005), the project's primary goals are to create a representation of international information and computer disciplines and to demonstrate the connections between different subject areas.

The project's output is intended for a wide range of applications, including curriculum development in educational institutions, program evaluation by accrediting bodies, program selection by employers looking for specialized skills, student assessment of their strengths and areas for improvement, and more. However, neither academic institutions nor businesses nor students were consulted for this project. Instead, the project will be carried out utilizing a Social Network Analysis (SNA) strategy, with the digital library serving as the main data source. It can take some time before this work is ready for evaluation because it is still in the development stage.

This study recommends using ontological principles for the organization of IT pedagogical information, as illustrated in Figure 2.3 above, in accordance with model curricula like IS 2002 (Gorgone et al., 2003) and MSIS 2006 (Gorgone et al., 2006) and other studies previously listed in this study. The IT-related curriculum and its relationship to other IT pedagogical concepts are conceptualized in this basic form. The Knowledge Hierarchy is shown in Figure 2.7 below, with other disciplines serving as a foundation and the IS curriculum situated at the upper right corner. Some IT experts, on the other hand, might adopt a more limited perspective and believe that IS only applies to the area indicated by region A (near the top right corner).

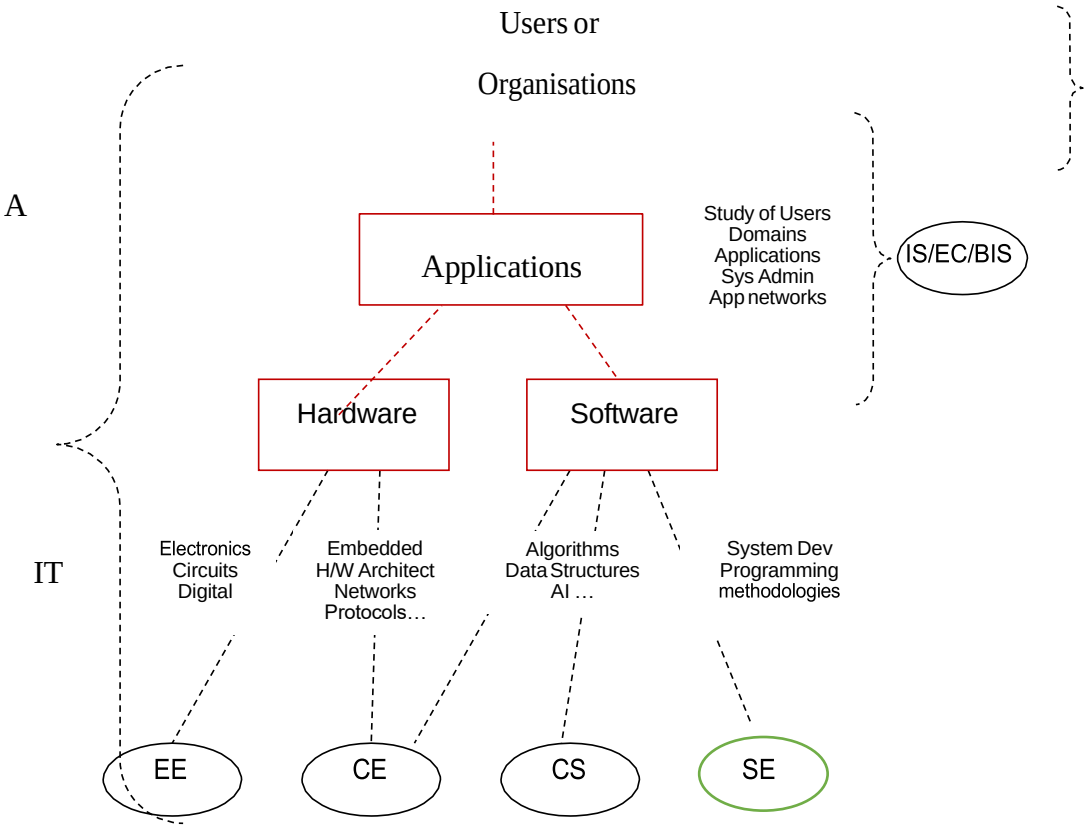

Figure 2.5 IT pedagogical Knowledge Hierarchy: An Ontological View, Endicott-Popovsky & Popovsky (2014).

It should be noted that Figure 2.6 depicts IT as including all computing-related professions. This is consistent with how the term "IT" is really used in business, industry, government, and commerce, where it is used to describe computer systems (software, hardware, or platforms) that support organizations and further their plans and goals (AS8015, 2005).

In general, top-down, or bottom-up methods can be used to construct a course. (Remember that a "course" in Australia is like a "degree" in the USA.) Subjects within a course must typically be determined before comprehensive organizational structures within each subject are added. However, several issues need to be taken into account, including:

various institutions may have various names for the same subject, or different organizations may use the same name for distinct subjects. There is a chance that a subject won't cover all the organizations it should or that comparable subjects at other colleges cover. A topic could not be in line with what the industry demands.

As a result, the suggestion is a layered ontology view of a pedagogical system that can be used with any IT-related curriculum. The system starts at the concept level, is organized into a

subject level, and then is finally organized into a course level, producing a layered ontology as shown in Figure 2.6 below.

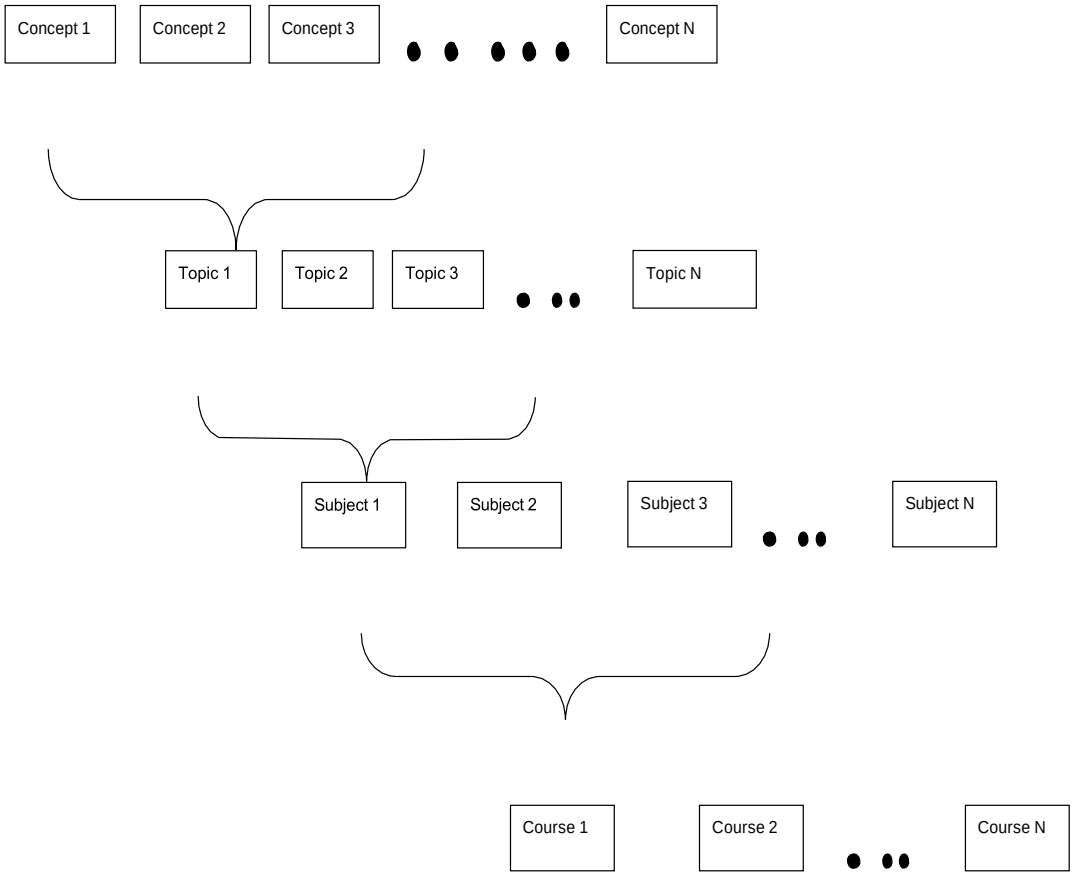

Figure 2.6 A pedagogical system is represented ontologically in layers (Endicott-Popovsky & Popovsky, 2014).

A curriculum is created by carefully defining Concepts and organizing them into Topics, as seen in Figure 2.8. Subject areas are created by grouping Topics, while Courses are created by grouping and sequencing Subjects. Academics, students, and industry will be the three key stakeholders considered in the detailed design of the collection of attributes for each element within the ontology to ensure that the ontology can satisfy questions from all three perspectives.

2.10.2. Why E-learning 2.0?

Because of the Internet's and the World Wide Web's quick development and widespread adoption, modern society has been somewhat unprepared for the digital economy that people now live and work in. In the past, big technical developments were often adopted and used at

a rate that still allowed society to progressively build responses to them (Manson & Pike, 2014). For instance, the broad adoption of the vehicle took place over several generations. This gave individuals time to create strategies for acting safely around and in autos.

As a result of this behavior being passed down from one generation to the next, a "culture" has developed in which everyone in society is aware of the risks that motorized vehicles may bring to their safety. The development of such a "culture" was not possible given the velocity at which the use of the Web permeated society. In addition to the fact that the original generation of online users is still in existence, technology is also still evolving quickly.

The recent emergence of social networking and other Web 2.0 phenomena is one of the best illustrations of how quickly new technology is being adopted in contemporary culture. Online learning communities would logically evolve to employ a similar strategy given that Web 2.0's participatory, collaborative, and dynamic online approach is arguably where most serious initiatives at Web-based development are currently headed (Manson & Pike, 2014). (2014) Manson & Pike. These innovative learning environments get learners ready for the real world by mimicking Internet users' habits. While it's accurate to say that some elements and organizational traits of the current educational system will probably prove durable as the preferred technique for learning organizations.

Web 2.0 trends will likely penetrate more of the educational system than one can now imagine (McGettrick, 2013). The resources that Web 2.0 offers the learning environment allow students to design their own knowledge structures rather than comply to the generic informational constructs that, for example, traditional education enforces. Educators offer the best potential outcome for the learning experience by letting students develop their information and store it in a method that is most effective and efficient for their learning style. A new breed of e-Learning systems called e-Learning 2.0 is the result of the fusion of Web 2.0 and e-Learning techniques.

E-learning has been proposed as a tool that could improve the effectiveness and efficiency of education and lifetime learning. However, the content that drives such systems is frequently static, and many e-Learning systems fail because they merely copy earlier educational paradigms (Mirshark, 2014). Due to how quickly IT changes and how frequently new technological developments are released, this is also true of many IT-related sectors. Researchers have had to reevaluate earlier e-Learning models in light of the development of social software on the Internet and the trend toward free educational resources. The phrase "E-

Learning 2.0" was first used in 2005 to refer to online e-Learning platforms that were created using social networking tools (Web 2.0) (Raytheon, 2014).

The Web as a medium, as it is well recognized and understood, is transformed into a platform for the distribution of data via this e-Learning system, a new style of learning that is profoundly anchored in the social constructivist paradigm (Raytheon, 2014). The delivery of content to students has evolved to include student authorship as well. Many authors view Web 2.0 as progressive and the main force behind the educational reform that is bringing new challenges and views to education at all levels.

Web 2.0 has many advantages for the educational industry, including its ease of publication, idea sharing, and reuse of study materials. Web 2.0 is viewed favorably by educators due to comments and links to pertinent resources in information environments that are run by the teachers and students themselves (Thaw, 2014). In contrast to earlier educational systems, where system developers employed study content creators who were tasked with creating a general knowledge base from which learners were educated, the idea of allowing learners the ability to manage and contribute to their learning environment (Eagle, 2013) is a novel one.

It may not always be the best learning strategy to require all students to access such a knowledge repository in the same way. One could argue that systems built on Web 2.0 might be more effective. While Web 2.0-based tools would allow students to spread out and pursue "informal" learning, previous information security education systems mainly focused on the usage of formal learning methodologies.

According to research, informal learning that takes place outside of the classroom accounts for between 80% and 90% of all learning (Eagle, 2013). Examples of computer program security were found to be particularly well-received by students in information security education, and informal explanations predominate over formal mathematical proofs (Gondree, 2016). Although informal learning design is nothing new, it has previously been disregarded by e-Learning designers (Pusey, Gondree, & Peterson, 2016). However, to date, little has been done to significantly change e-Learning design processes to embrace more informal learning techniques (Razana & Shafiuddin, 2016). Organizations themselves ought to be sufficient to make this happen. Therefore, it is important to look at the implementation of such a system for information security education to determine whether it will be helpful in training all computer system users worldwide.

As was argued before, people from various walks of life now use computer systems in an organization in addition to ordinary adults. Information security education must therefore move

beyond organizational information security and toward cyber-security education that targets all of these potential victims. It might be claimed that E-Learning 2.0 systems are most suited for this role since they are Web-based platforms that make use of technology that these potential learners are already exposed to through other activities.

The user can "Rip, Mix, and Feed" using e-Learning 2.0 platforms, which enable users to participate as both consumers and producers (Endicott-Popovsky, & Popovsky, 2014). By using this method, multiple people can contribute to the creation of educational content rather than just one or two. As a result, the development of the information security education content base turns into a collaborative effort that necessitates the implementation of a number of grading systems to assess the reliability of the writers and the output of such a collaborative effort. The student is guaranteed a sense of ownership for the content they produced by allowing them to not only draw from but also add to the content base. Giving people a sense of ownership stimulates their desire for more education, which in turn inspires them to advance their education and become better people. By forcing the learner to integrate and maintain the social software tools that enable the learning to occur, the system actively engages the learner in the learning process (Salend, 2015).

The wide and sophisticated benefits of e-Learning 2.0 systems enable these systems to quickly replace many of the traditional learning methods already in use. As a result, this study makes the claim that using E-learning 2.0 for "cyber-security education" may be the best method to handle the growing demand to give students from all walks of life the knowledge they need to be "safe" online. Unfortunately, the benefits that come with such "revolutionary" educational technology are also accompanied by several difficulties that could impede the growth and effectiveness of such systems. The next part will provide a brief analysis of the most prominent of these difficulties.

2.10.3. Problems with Learner-Generated Learning Material

The encouragement of learner-assisted content development and dissemination enables the generation of a wealth of data on various organizations involved in cyber-security. Another potential issue arises because of the production of such massive amounts of information. First, learners may experience information overload rather than a lack of adequate information security material (Cain, 2010). The fact that it takes a long time and a lot of money to develop a proper knowledge base from which to educate learners was one of the issues with old e-Learning systems. Experts in the field who provide content as part of their jobs are often those

that produce the courses for information security education systems. A system based on "folksonomy" is created by e-learning 2.0, which enables the students themselves to contribute and enhance the learning materials.

This has a lot of benefits, but it also raises the possibility of information overload. When a learner searches for a specific topic, too much information is returned, making it difficult for the learner to manage and sift through it to find the desired topic (Asiimwe, 2010). If learners are not restricted to the scope of a contribution, certain information security organizations may have a large amount of content associated with them. Second, a system to guarantee the accuracy of learner-generated content would be necessary to secure its widespread adoption. Due to the lack of such controls, the accuracy of the information found at sources like Wikipedia is sometimes questioned. Concerns about the trustworthiness, dependability, and plausibility of learner-created content in general are raised by detractors (Breibart, 2010).

Any proposed system must provide efficient management of a huge volume of uploaded material in order to optimize learner searches and return only information relevant to a given search. On e-Learning 2.0 systems, this is still challenging to do because each kind offers a unique capability for storing knowledge that is private and has a different architecture from other similar applications. This means that for one system to exchange content with another system, it would have to expose its knowledge store's API to the outside world and need the receiving program to create custom code in order to communicate with it. The number of apps that can communicate with one another would be significantly constrained if this kind of code had to be developed for each remote knowledge store that the receiving application desired to connect with. The Semantic Web, which is now under development and is quickly gathering steam as the next step in the Web's growth, is one potential answer to this issue.

2.10.4. Towards Information Security Education 3.0

Web 2.0 made the Web accessible and let regular computer users contribute information. Although it addressed the issue of content generation, this contribution facility also created other issues that needed to be resolved to guarantee the Web's success going forward and support its rapid expansion. Information overload is one issue with enabling contributions from numerous sources. It is typically highly challenging for machine users (or apps) to comprehend the information uploaded and derive conclusions from it since it is typically stored in a format that is only appropriate for human readers. As a result, computer users and software programs are unable to comprehend information security concepts and the contributions that users of the

system make. Concepts in information security education would not necessarily be machine comprehensible, even though machines could read them (Ctftime, 2017). Machine users must be able to digest the information and comprehend its contents to enable searches that reliably and efficiently filter through all of this information, minimizing information overload for system users. According to Koehler (2017), the Semantic Web can be compared to a massive relational database that connects tagged items and includes all types of organizations and concepts, from book chapters to mobile phone prices to laptop computer prices. The Semantic Web allows information created by students on an information security education system to be transformed from a "display only" form, only passable by humans or software agents have written specifically for the task, to a vast database of knowledge, which computer applications can parse and understand (Zain, Sahimi, Hanafi, Halim, & Alias, 2016). This is done by joining these organizations in a way that computer applications can understand. With this knowledge, computers may more correctly search for specified criteria inside the information security education system's content base and handle a large portion of the labor-intensive information processing and filtering required for queries made by system users. Users can also discover connections between items that are marked, such as linked information security organizations, using the Semantic Web (Tan, 2015). The Semantic Web's capacity to use ontologies, which are domain theories and data organization tools, makes it possible for a Web to provide a qualitatively new level of service (Hemingway & Gough, 2010).

Gruber (2013) defined an ontology as a formal and clear specification of a common conceptualization. Formal, i.e., it should be expressed in a formal representation language, and shared, i.e., it should be understood by everyone (McKenzie, 2016). Ontologies' main objective is to make it easier for people to share and reuse information by giving individuals and applications on the Semantic Web a shared understanding of various types of content (Mocan, Cimpian, & Kerrigan, 2006). Only if there are numerous ontologies around these systems can learning systems on the Web that exchange domain and pedagogical knowledge function (OntoWeb, 2002). This is not the case now because there aren't many domain ontologies, and even fewer that cover learning theories and instructional design (Mitnick & Simon, 2013). For this reason, the learning community in general, and in this case the information security educational community specifically, needs to come together and collaboratively develop the standard ontologies, much like the contributions to a wiki, where all users input is valued by the community working toward a common goal and is condensed and refined by the community.

The apparent lack of a common lexicon in the fields of education and instructional design is one of the primary causes of the lack of such standardized ontologies for learning (Wamala, 2011). These and other challenges are being addressed by numerous standards bodies. However, there is currently no organization focused on developing ontologies for information security education.

According to the debate above, information security education is required outside the walls of contemporary organizations. People from all areas of life use the Internet as a tool for communication, entertainment, and a variety of other tasks. To help shield them from the risks associated with participating in such activities online, it is necessary to educate these people. Such instruction ought to be presented in a way that motivates respondents to participate voluntarily. Utilizing the Web 2.0 philosophy to involve such learners in the collaborative creation of educational content is one option to consider. Numerous educational academics have proposed the idea of such an e-learning 2.0 strategy, but its efficacy has not yet been established. However, subject-specific ontologies for the targeted subject matter would be required before such an approach could become a reality.

2.11. Information Assurance Security Educational Model for Information Technology Curricula in South Africa

Four significant American organizations have created guidelines for computer courses for colleges and universities during the past few decades. Association for Computing Machinery (ACM), Association for Information Systems (AIS), Association for Information Technology Professionals (AITP), and Computer Society of the Institute for Electrical and Electronic Organizations Engineers (IEEE-CS) are a few of these organizations (Ophardt, 2010).

Future Information Technology (IT) workers are being trained through the Schools of Information and Communication Technology (ICT). It does not get any special curriculum recommendations, nevertheless, to guarantee that all crucial security-related topics are included in the IT courses that are available. The educational offers that must be included at each level of the curricula are governed by the South African curricula requirements for IT qualifications (Ophardt, 2010). They do not, however, offer detailed instructions regarding the suggested material. They are consequently forced to self-regulate by evaluating their performance against global norms and standards, similar to several South African institutions. The ACM/AIS/IEEE-CS Computing Curricula 2005 is one such standard for the computing industry (Hildreth, 2001). In the document "Information Technology 2008, Curriculum Guidelines for

Undergraduate Degree Programme in Information Technology" (Hua & Bapna, 2012), the ACM/IEEE-CS offers such a standard for the IT industry.

This thesis argues that the curricula standards from the South African Council for Higher Education (CHE) and the ACM/IEEE-CS do not provide enough direction to guarantee that information security is appropriately incorporated into the IT curricula of the School of ICT. In order to handle IAS as a topic that is present throughout IT courses, it also suggests an integrated IAS educational paradigm.

The recommendations' impact on IT, curriculum designers, and educators at South African universities is discussed in the parts that follow. This is followed by some pertinent criticisms and recommendations.

2.11.1 Curriculum Guidelines for Undergraduate Degree Programme in Information Technology

The ACM/AIS/IEEE-CS Computing Curricula volumes' most recent academic discipline to be covered is IT (Hua & Bapna, 2012). ACM/IEEE-CS lists programming, networking, human-computer interaction, databases, and web systems as the foundations of IT. These are constructed upon a knowledge base of IT principles. Information assurance, security, and professionalism serve as the overall foundation's pillars.

A curriculum for a 4-year IT degree program is presented in "Information Technology 2008, Curriculum Guidelines for Undergraduate Degree Programme in IT" by the ACM/IEEE-CS. By doing this, it establishes a body of IT knowledge that covers 13 different subject areas. The knowledge area known as Information Assurance and Security (IAS) belongs to this group. These knowledge domains are then broken down into more manageable parts, each of which stands for a distinct subject within the relevant domain. Each unit is grouped into a group of pertinent organizations at the base of the organizational structure.

According to the ACM/IEEE-CS curriculum recommendations, IAS is a knowledge area that is well defined. It is acknowledged as a very interdisciplinary field of study, and all senior IT students ought to be involved. Every student should be involved with some of the advanced security outcomes, according to ACM/IEEE-CS, which also argues that "every student needs some advanced, integrative experience in IAS in the fourth year." Fundamental Aspects, Security Mechanisms, Operational Issues, Policy, Attacks, Security Domains, Forensic Organizations, Information States, Security Services, Threat Analysis Model, and Vulnerabilities are some of the units that make up this knowledge area. IAS should receive

about 7.5% of the total core hours allotted for the four-year program. There is a fear that certain university curricula would only include security-related topics at the fourth-year level because much of the information designated by IAS as a knowledge area may be seen as primarily geared at this level. Additionally, because it is a specialized topic of study, it might be recognized as an optional at some universities. Since numerous security units are described within other knowledge fields, the ACM/IEEE-CS (2017) solves this issue to some extent. Information assurance and security are generally covered in some detail in the knowledge areas of IT Fundamentals (ITF), Information Assurance and Security (IAS), Information Management (IM), Integrative Programming and Technologies (IPT), Networking (NET), Platform Technologies (PT), System Administration and Maintenance (SA), Social and Professional Issues (SP), and Web Systems and Technologies (WS). Software security procedures, for instance, are covered by the Integrative Programming and Technologies (IPT) knowledge area, while the Networking (NET) knowledge area has a specified security unit. Additionally, the Web Systems and Technologies (WS) knowledge area lists Vulnerabilities as a unit. However, there are no security-related topics covered in the knowledge domains of Human-Computer Interaction (HCI), Mathematics Organizations and Statistics Organizations for IT (MS), Programming Fundamentals (PF), and System Integration and Architecture (SIA). IAS is a recurring theme in ACM/IEEE-CS 2017, as will be covered in the next section.

2.11.2 IAS as a Pervasive Theme

IAS has been described as a ubiquitous motif in addition to being a key knowledge area. Those organizations that are "considered essential, but that did not seem to belong in a single specific knowledge area or unit" are referred to as a pervasive theme by ACM/IEEE-CS (2017). As a result, these topics ought to be covered frequently and in various classes as part of the curriculum. Under IT Fundamentals (ITF), the overarching principles of the IT curriculum are presented. According to the ACM/IEEE-CS, all pervasive IT themes must be covered by the end of the four-year curriculum and must be addressed often from the first to the fourth year. IAS is a knowledge field and a widespread concept, yet at other universities, it might not even be brought up until the fourth year.

According to the ACM/IEEE-CS definition of the IT body of knowledge, IT Fundamentals (ITF) should occupy about 8% of the core IT curriculum hours. 'Pervasive Themes in IT' should make up nearly 68% of this 8%, or roughly 5.5% of the total core hours specified for the 4-

year curriculum. How much time should be devoted to IAS as a prevalent subject, however, is not further broken down. This implies that IAS may not be given priority over other organizations in the "Pervasive Themes in IT" unit. This could result in an IT graduate leaving school with apparent knowledge gaps in security.

The IT Fundamentals (ITF) knowledge area is meant to be at the introductory level of a curriculum, according the IT curricula recommendations of the ACM/IEEE-CS. The ITF knowledge area's goal is to help students acquire fundamental abilities for later courses by giving them a general understanding of the IT discipline and how it relates to other disciplines. This should assist IT students comprehend the various contexts in which IT is utilized by fostering an IT perspective (Futcher et al., 2017).

The four units that make up the ITF knowledge area. 'Pervasive Themes in IT', 'History of IT', 'IT and its Related and Informing Disciplines', and 'Application Domains' are a few of these units. The 'Pervasive Themes in IT' unit also includes IAS as a topic. The basic learning objective, "Explain why the IAS perspective needs to pervade all aspects of IT," is linked to IAS as a topic.

These recommendations from ACM/IEEE-CS are used informally by several South African colleges when developing IT curriculum. The authors believe that these guidelines fall short in addressing IAS as a pervasive topic and that no additional guidance is available to help IT instructors create curricula that successfully incorporate IAS into the undergraduate curriculum. Futcher, Schroder, and Von Solms (2017) challenge the degree to which information security is integrated into the IT/IS/CS curricula at South African universities as evidence for this claim.. They express worry over the inadequate undergraduate attention given to information security and propose that information security be designated as a key cross-field outcome (CCFO) in South African curricula recommendations. This suggests that security-related topics be covered in the first year of study of the IT, IS, and CS curricula. In keeping with this, the following section compares the ACM/IEEE-CS recommendations with the curriculum currently used in South Africa (Futcher et al., 2017).

2.11.3. Evaluation of South African Curricula Guidelines Against the ACM/IEEE-SC

For tertiary institutions, the South African Higher Education Council (CHE) provides guidance on the organization of curricula. The recommendation is still present in documents from the

National Assembly of the Department of Training and Education (NATED), the South African Qualifications Authority (SAQA), and the Credentials System for Higher Education (CSHE). This section examines the guidelines provided by the CHE for IT qualifications in order to unbiasedly evaluate them in comparison to the ACM/IEEE-CS curriculum requirements (Department of State Security, 2012). The objective is to identify potential weaknesses and solutions to improve how information protection might be incorporated into IT courses. A uniform framework for a broadly integrated field of higher education, the CSHE. All services and certifications offered by South African public and/or private organizations are included. This means that it does away with earlier political documents like "Southern African Qualification Structure - NATED report 116 (99/02)," "Technikon Instructional Program General Strategy - NATED report 150 (97/01)," and "NATED Report 151 (99/01) Structured Technikon Instructional Programme." The NATED records do contain some significant educational materials, though.

The National Certificate and Bachelor of Science in Computer Technology programs are highlighted in NATED Study 151 (Nicholson, Webber, Dyer, Patel, & Janicke, 2012). The Bachelor of Technology credentials are included for Computer Security IV and Information Security IV even though there are no obvious security offers for the National Diploma. Therefore, none of SAQA's nine advanced IT domains require these two deals (Wolf Pack, 2012). Enterprise applications, software development, communications networking, site and application development, knowledge and technology management systems, intelligent manufacturing systems, support facilities, hardware and technical solutions, and computer architecture are some of these fields.

For the SAQA's National IT Diploma, none of these IT-related categories have any unique or protected results (Cisco, 2019). The SAQA registered IT Technology Bachelor [3], which assigns an exit level related to safety to each of the nine IT areas, states that "the learner should be able to use advanced technologies to enforce and monitor information protection in an IT environment." It is only included as an option for the other eight IT fields and as a core for the area of business applications. This outcome standard is linked to the associated evaluation criteria, "Evaluation of the computer protection system and design control measures." This raises serious questions about IAS's place as a major issue in South African IT courses.

Additionally, the ACM/IEEE-CS program standards offer a fantastic structure for developing a 4-year IT program. In particular, it suggests including IAS as an advanced subject in the

fourth year and provides very strong recommendations on prestigious companies that such a training offer might contain. However, the first three years of research and the surviving top organizations in the fourth year show a general tendency of a lack of precise guidance about how to execute protective principles.

Future difficulties could result from this on several levels. First off, it would seem that an optional certification is offered during the fourth year of study given the nature of the several 4-year IT programs and the variety of associated South African colleges (Choo, 2011). As a result, following the third year of studies, a student may drop out of the certificate program. Second, the "Information Security" educational offer is considered optional by the South African curriculum guidelines, except for students who choose to apply for the fourth-year optional certification. Then, students may decide not to participate in the required computer security training. As a result, given the relative importance placed on this subject in the ACM/IEEE-CS (2017) curriculum guidelines, IT curricula that do not adequately address information security may result from a lack of detailed instructions about how the information protection principles should be implemented in subject curricula during the first three years of research.

While it is unfair to demand that the ACM / IEEE-CS contain comprehensive instructions on these topics, it has been suggested that the Curricula Recommendations should more precisely set minimum "standards" on this potential area of concern. As suggested by Van Niekerk and Von Solms (2017), this can probably be achieved by leveraging the Information Assurance model included in the ACM / IEEE-CS Guidelines to incorporate the framework for the security of the information and usage of a learning taxonomy like Bloom's taxonomy.

For instance, the topic "buffer overflow attacks/prevention" should not only be a fourth-year topic that is optional. Instead, it could be added during the programming qualification. Thus, using a study taxonomy like Bloom's, specific learning objectives may be set that require students to remember and recognize the materials on this subject in their first and second years of study and to be able to apply the information they need in their third year.

Even with the proposed information assurance model included this subject's entrance into the programming program may involve a protective framework. As a result, according to the underlying facts, protection resources and/or countermeasures that are crucial to the way that some subjects are taught may also be related.

Only the lowest three levels of Bloom's taxonomy are covered in Table 2.6's brief samples of sample learning activities for the topic of "buffer overflow attacks/prevention". The remaining levels may also have similar examples built but were left out for space reasons.

Level	**Verb**	**Sample Activities**
Apply	execute	Write error prevention code to ensure that your methods iterating through the given list of stored items cannot overstep the boundaries of this list. (Security Countermeasure)
Understand	discuss	Explain how the integrity of the data in the computer's memory could be negatively affected if your code tries to access an array element outside the boundaries of the current array. (Security Services)
Remember	define	In terms of the underlying memory used/allocated, define what an array of 32-bit integers is. (Information States)

Table 2.6. For information security, a condensed example of learning activities based on Bloom's Taxonomy (Anderson et al., 2016).

This incorporation of Bloom's taxonomy into the planned curriculum design process might also be reflected in the information assurance model proposed by ACM/IEEE-SC (2014). Like an earlier modification, "Time" was introduced to the model as a fourth dimension by Maconachy, Schou, Ragsdale, and Welch (2018). Time was introduced, however it wasn't treated as "a causal agent of change, but a confounding change agent" (p. 9). This addressed the requirement to adjust other dimensions to accommodate evolving technologies.

Similar to the adaptation shown in Figure 1, it is not a causal agent but rather serves to highlight how, according to Bloom's taxonomy, a student's understanding of fundamental, pervasive security concepts grows as he or she moves through the course material. Therefore, a student might initially only work with a certain concept at the cognitive domain's "remember" level but should eventually advance to the "create" dimension.

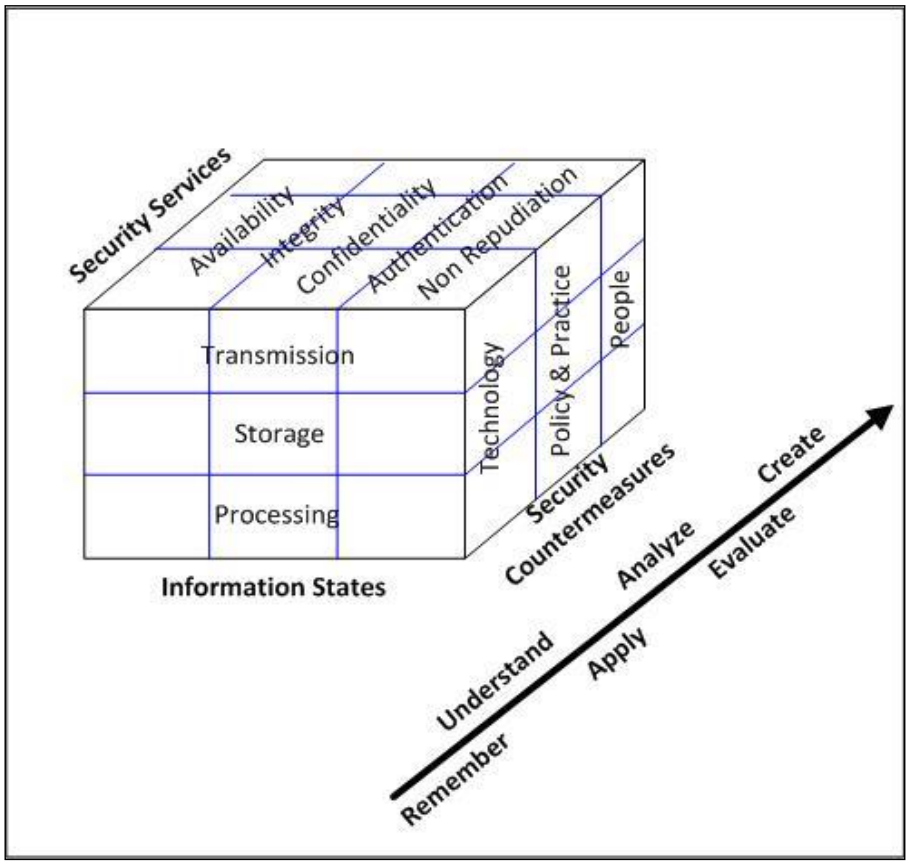

Figure 2.7: (Maconachy, et al., 2010) Model for Pervasive Information Assurance and Security Education

There are difficulties specific to the IT industry in integrating many of the IAS ideas into the curriculum. This problem may be helped to solve by the proposed paradigm for pervasive information assurance and security education shown in Figure 2.6.

In summary, even while the ACM/IEEE-CS supports IAS as a field of study and a large subject, not much guidance is provided to help IT educators use IT protection as a broad theme in their numerous resources. At the national level, more guidelines on the ACM/IEEE or the IAS as a general theme should be offered. It will be beneficial to "level" concepts using a learning taxonomy in order to integrate IAS into IT curriculum as a whole. The basic, important, and optional security issues to be incorporated into IT credentials from the first to fourth year will be decided by curriculum authors and teachers through the implementation of the proposed overall IT information assurance and protection model. Although the fundamental basis should form the core of the certification proposal, the major elements should necessitate rigorous preparation under conditions unique to the training offer. Elective thoughts ought to offer a few fresh security points that might strengthen certification. Both the ACM/IEEE-SC and CHE recommendations will be helpful for implementing the suggested paradigm.

Finally, CHE lacks comprehensive topic-level instruction. According to the authors, South African IT instructors should formally adopt the ACM/IEEE-ORGANISATIONS guidelines until detailed instructions are provided. However, the authors believe that in order to include security as a general concern, considerably more clarity is needed from a security perspective. Therefore, further research is required to determine whether security-related issues are addressed in the institutional learning programme's guidelines.

2.12. Justification of Cyber security Education curriculum

Many of us use social media as a platform to communicate our thoughts, start conversations, or establish our identities. Many people often disregard whether the information supplied is accurate or not because they want to be the first to address a problem [1]. In this day of technology and multimedia, not only do adults utilize the internet, but youngsters also need to be aware of cyber security. Even if the Internet has enormous potential and advantages for everyone, excessive Internet use may be dangerous since it increases the chance of cyber hazards such cyber addiction [2], gaming and gambling addiction [3,], cybersex [4,], pornography [5,], and exposure to personal information (Ciampa, 2015).

Parents are understandably concerned about cybercrime against children and teenagers because, on occasion, they are unaware that their child has been a victim. Many parents are ignorant of the online activities their kids engage in. Some kids experience verbal and physical bullying, as well as intimidation, harassment, abuse, and sexual exploitation. Nearly 80% of rape cases reported in South Africa over the previous two years, according to police records, involved online friendships, and most of the victims were under the age of 18 (Brown & Wang, 2011). The problem of grooming children and teenagers to become sexual abuse victims is getting worse as more and more sexual predators use false identities online to look for victims.

There is no denying that children are adept and skilled considering their young age when using their smartphones or smartphones, despite parents' efforts to protect them from cyber-attacks. Children are proficient in technology as well as tech-savvy. Some parents give their kids gadgets as prizes for tests, as birthday presents, etc. Young children are thus vulnerable to electronic violence when using the Internet unrestricted or unsupervised. When children have access to the internet at a younger age, it is crucial for everyone—parents or kids—to be aware of potential risks like cyberbullying and to take safety precautions if you value the benefits of the internet (Ayers, 2010). Educators should spread cyber security lessons to promote safe online behavior (Brown & Wang, 2011).

The way that children use the Internet is fast changing in response to significant social, commercial, and technological advancements. Children frequently interact with online photos, songs, games, messages, and searches, which indicates that their internet usage is generally positive. Parents of children aged three to four say that their kids probably enjoy watching cartoons, short movies, animation, or music on YouTube. The quality of children varies as they become older because older kids watch more movies, vloggers, YouTube personalities, and funny videos (Brown & Wang, 2011). Schools have an important responsibility to teach kids essential digital literacy skills as well as to counsel and inform parents about how to use the Internet at home with their children.

The goal of cyber security education is to inform computer users of the potential risks they may face when using services like social networking, chat, online gaming, e-mail, and instant messaging. While numerous studies have been conducted in the past on cyber protection in a variety of disciplines, such as (Bui, 2014), there aren't as many publications as possible that focus on the steps that institutions, particularly schools, should take to support the development of a thorough awareness of cyber-security. In light of the distinctive characteristics of the South African educational system, the aim of this article is to discuss why it is so crucial to educate contemporary students about the risks of engaging in cyberspace, what factors are impeding this education, and the importance of a Cyber security program for junior or primary school teachers.

Due to the development of the internet, consumers can now enjoy both the real world and the virtual one (Bui, 2014). People can now access this content via search engines like Google and Yahoo as well as video-sharing websites like YouTube. However, even the growing area of cyberspace, like cybercrime, could have negative effects on internet users. Therefore, it is important to address those worries before they have a substantial impact. In this view, the implementation of cyber security is crucial for internet users.

According to Davis, Leek, Zhivich, Gwinnup, and Leonard (2014), the idea of cyber security indicates that a state is protected from, or measures are made to achieve, the illicit or criminal use of computer data. Our lives have dramatically improved because of the proliferation of ICT. Individuals and organizations can easily examine some details thanks to the World Wide Web's preservation, but if it were utilized for evil, it would negatively affect the lives of residents (Evans and Reeder, 2010). Additionally, the internet offers pornography that can contribute to societal problems like violence. Given that Malay teenagers are the main source of the school truce, the Internet may also be a dangerous conduit for violence and corruption.

According to Davis et al. (2014), cyber security can also be defined as a method, capability, or state that offers safety from injury, illegal access to, alteration of, or manipulation of information, communications systems, and their contents. The Internet without a doubt improves one's consciousness. To understand the setup and rules of an online video game, for instance, respondents must be fluent in English. Implicitly, this will help to develop readers', writers', and speakers' abilities in English. The average video game, however, is entertaining and takes the player a long time to complete. Teenagers may become indolent or reliant on video games and technology as a result. Adolescents are prone to becoming dependant, and helpful actions like reviewing their lessons are frequently overlooked.

Reports of cybercrime and cyberromance schemes, best known as the African Scam, are concerning (McKinsey, 2016). In South Africa, there were 1095 more internet fraud instances in 2016 than there were in 2012 (814). McKinsey, (2016) also references an incident involving an 18-year-old South African minor who was charged with violating the 1987 Copyright Act for duplicating local music and foreign films without the owner's consent. include The Hobbit: Smaug's Desolation, Gravity, Pacific Bottom, 47 Ronin, The Hangover III, We Are the Millers, Travel Along, and The Wolverine. According to McKinsey (2016), illegal online transactions increased in Malaysia in 2015, costing the automotive, real estate, and tourist sectors more than R14.9 billion.

Getting ready for cyber security is frequently necessary to control video game addiction. This dependence has a negative impact. Young folks spend a lot of time on laptops for socializing. Video game addiction becomes uncontrollable over time, and device addiction steals young people's important free time. Teenagers are severely harmed by this. Spending too much time on the phone at night makes the problem worse and could potentially affect young people's health. Consumers are frequently unaware that they are being threatened in these threats and assaults, which can happen in a variety of situations. In order to foster a culture of cyber safety, it is vital to inform and inspire users—especially young people—to utilize online services and platforms responsibly (Ciampa, 2015).

Finally, the market is possibly the biggest obstacle here, particularly among CEOs and boards. Decision-makers are unaware of the risks to cyber safety and the costs of addressing them. According to a poll by the Economist Intelligence Unit, less than 6% of the C-Suite executives in Australia agree that cyber security is currently the country's top issue. Between the reality of hazards and how they are perceived at the executive level, there is a significant gap (Ciampa, 2015).

2.13. Challenges of Cyber Security Education

The demand for trained ICT positions will increase from 638,000 today to 695,000 by 2023, according to a study conducted by Cisco (2019), with ICT graduates only meeting 1% of the requirement. In contrast, the number of ICT disciplines reported by universities has decreased by 35% since 2001.

Before moving to an information economy, more physicists, mathematicians, developers, and programmers would be needed. A rising emphasis on entrepreneurship skills, the development of university-based degrees in cyber safety, and the promotion of STEM subjects in the classroom can all assist to track the contribution of South Africans to the ICT industry.

It's interesting that while certain professionals, like lawyers and doctors, are respected, there are differences in the education and experience required to become a cyber security specialist. But we're already at a point where qualified cyber security professionals are essential to the operation of most South African businesses. It is necessary to create a profession that is valued equally to other highly trained jobs. Data protection is frequently integrated into training programs since, as was already mentioned, an organization's activity has the strongest connection to its cyber security policies and strategies.

In South Africa, social networking websites including Facebook, Instagram, LinkedIn, YouTube, and Twitter are the most widely used Internet applications. There are many concerns to privacy and protection as a result of this knowledge flow. In this participatory setting, the accuracy and quality of the details can also be questioned. Children need to be taught how to defend themselves and accept responsibility for potential cyberattacks. Additionally, it can be challenging to ensure that teachers are adequately trained and up to date so they can guide kids and parents in their use of the internet at home while fostering critical thinking rather than conserving attitudes toward computer security.

The multiple problems that school face in cyber security education include a lack of infrastructure, support, and skill sets (Van Niekerk & Von Solms, 2006). Skills and experience in online are neglected by teachers. Infrastructure and facilities for schools and government departments will be inadequate for cyber security education. The speed of technological progress creates new risks and calls for fresh thinking. Teachers will struggle to create the new technology and ensure student safety as a result. Teachers face a significant problem in this situation because they lack access to educational resources and are sensitive to technological advancements. Symposia on computer security can be used to encourage early awareness and

preparation among students. The nation's prospective cyber defense source is projected to be people who are exposed to and educated about cyber protection.

Finally, the market is possibly the biggest obstacle here, particularly among CEOs and boards. Decision-makers are unaware of the risks to cyber safety and the costs of addressing them. According to a poll by the Economist Intelligence Unit, less than 6% of the C-Suite executives in Australia agree that cyber security is currently the country's top issue. Between the reality of hazards and how they are perceived at the executive level, there is a significant gap (Ciampa, 2015).

2.14. Conclusions

Since the field of cyber security is expanding quickly, there is a demand for more knowledgeable, well-trained employees. The demand for cyber security specialties is one of the strategies that educators must use to prepare this workforce. The reviews, which were based on a holistic paradigm, thoroughly considered the seven variables that affected our choice to offer three specialties in the Cyber security programs: data analysis for cyber security, cyber intelligence, and privacy and security in healthcare. A review of the selected literature revealed that it is crucial to educate people about cyber security in order to safeguard systems from potential threats when they use online communication tools like social networking, chatting, and online gaming. But teaching cyber security faces a number of difficulties. These include the knowledge of teachers, as well as a lack of resources, finance, and competence. In order to safeguard children from cyberbullying and cybercrime, it is crucial that all involved parties—teachers, parents, classmates, and the government—work together to develop the most effective solution. Because these campaigns are more interactive and fascinating for children to understand, the media, such as television and radio, must also play a significant role in educating children about cyber security.

CHAPTER 3

THE THEORETICAL FRAMEWORK

3.1. Introduction

The IT degree program is not intended to teach any single topic in detail, but to provide a wide spectrum of expertise and skills, which results in a fully-fledged IT potential specialist from entry-level. Like with many IT programs, students are expected to work to apply the most recent technology, get extra training from their team, and pursue more expert education or certifications if applicable. This requires following acclaimed procedures of curriculum development as well as pedagogy so that objectives can be achieved.

The objective choices teachers make for their students are related to the reasoned component of education. The purposeful part of teaching focuses on how instructors support learners in achieving instructors' goals, which includes designing learning settings and offering relevant activities and experiences. The learning settings, activities, and experiences should be consistent with the chosen objectives or be in alignment with them. From the above, this chapter explores the revised Blooms' taxonomy of teaching and learning especially in curriculum development, teaching and learning with reference to ICT.

3.2. Framework for theoretical information security instruction

IT has become such a crucial component of contemporary business in recent years that several authors no longer consider its usage to be a technique. Instead, it is possible to claim that information technology is only a utility, like energy, and that a lack of it makes it challenging to work (Carr, 2003). Additionally, organizations must ensure that they have ongoing access to this valuable resource. Records protection is the process of preserving this ongoing access.

Individuals at all levels are essential to the procedures that safeguard the company information capital. Many information management problems can be traced back to the people involved in the process. Because of their lack of experience, employees pose the biggest threat to information security, both intentionally and unintentionally (Mitnick & Simon 2002, p. 3). Organizations that care about protecting their information resources must also carefully consider investing in employee training. To guarantee that every person in the organization

understands their responsibility for the security of information should be the main objective of corporate information management education.

The idea of informing corporate customers of their responsibilities and roles in information security is also widely known. The most pertinent security information requirements provide a solution to this demand. In a highly networked device environment used on a daily basis, for instance, ISO / IEC standards 13335-1 state that organizations cannot protect information privacy, secrecy, and availability without ensuring that each user shares an organization's security strategy and is aware of and properly trained for their roles and responsibilities. Individual users must understand their role in the security process as well in order to effectively assure information security. Initiatives for education, training, and awareness can produce this knowledge.

The most current educational information security initiative consists of information security professionals who are not generally trained. Puhakainen (2016) reviewed 59 emerging threat knowledge techniques, most of which were not pedagogical. Puhakainen (2016) also argues that theoretical security methods are important. These methods can also be realistic. The essence of protection education or awareness-raising problems, which can lead to initiatives and recommendations that are unsuccessful in operation, are also not understood (Siponen 2010).

For example, a formally qualified educationalist might ask whether the information is appropriate. Only the very first and lowest educational standard is included in the data according to Bloom's taxonomy, a well-known and widely accepted pedagogical taxonomy (Sousa, 2016). One might argue that this degree of awareness is not appropriate for most individuals who are interested in the process of information security. Likewise, the conventional way to classifying the required educational information security requirements as a continuum to knowledge, schooling or training can also be too simplified.

3.3. Awareness, education, and training in information security

As previously mentioned, most of the current research on information security education views this training as a continuum of learning that starts with comprehension, develops training, and culminates in knowledge (NIST 800-50, 2017). The following levels are defined by NIST 800-16 (2018), which describes the various phases of the spectrum.:

Awareness: Programs for education are generally designed to inform personnel about information security. These campaigns therefore depend on health. This is often accomplished with techniques that aim for large audiences. Sensitization campaigns are usually targeted at any employee in the company and seek to provide workers with adequate information to detect possible security risks. Sensitivity is not preparation.

Training: Training is more systematic than empathy and is meant to develop staff awareness and skills to allow workers to carry out their usual duties safely. Education aims to improve security expertise and skills that are important to workers and required in the execution of their duties. “While awareness works to draw people's attention to a topic or set of issues, training focuses on giving people the skills necessary for a certain function.” (Siponen, 2000).

Education: To produce IT security practitioners and experts who can provide direction and proactive solutions, the standard of training integrates all protection skills and abilities from different practice areas into a single body of knowledge. It also combines a multidisciplinary analysis of concepts, challenges, and values (in technology and society).

Education or literacy issues concern nearly all organisations in the modern information society. However, the essence of the program is still not fully known, which also leads to inadequate safety manuals or services (Siponen, 2000). Many organisations provide a type of awareness programme, but often do not increase this with funding services for training and/or education. Education and sensitivity are frequently used synonymously. Security analysts frequently discuss awareness campaigns as they focus on the spectrum stage of education or training.

These initiatives always seek to promote safety consciousness or a culture of information protection among end users within organizations (Van Niekerk & Von Solms, 2006). Information just de-writes the lowest level of Bloom's taxonomy of cognitive domains, as was previously mentioned. In terms of schooling, it may also be argued that the language used is not rigorous. This lack of rigour may lead to the sometimes misconception of the essence of awareness and education. Bloom's taxonomy is a model that might potentially have some rigour.

By incorporating the revised Bloom taxonomy (Anderson et al., 2001) as a pedagogical structure, based on their individual roles and responsibility for security, this study aims to understand the instructional needs of people involved in information security systems.

3.4. Bloom’s Taxonomy for information security education

A classification of learning stages based on intellectual behavior, known as Bloom's Taxonomy, was created by Benjamin Bloom and a group of academics in 1956 (Bloom and Krathwol, 2002). The taxonomy's core components underwent an upgrade in 2001 to better align with the educational objectives of the twenty-first century (Anderson and Krathwohl, 2001; Krathwohl, 2002). Norman Webb created a method to evaluate how standards and standardized tests correspond in 1997. The Depth of Knowledge (DoK) Model, a procedure, is also used to examine how well curricula connect with standards and assessments (Webb, 1997). The model assumes that expected student behaviors within courses can be grouped according to the cognitive demands required to generate appropriate replies. Each grouping of tasks illustrates a particular degree of information or amount of cognitive expectation needed to perform the tasks.

When creating specific student learning outcomes, as shown in figure 3.1, it can be helpful to combine the elements of the updated Bloom's Taxonomy with the categories for depth of knowledge from Webb's DoK Model (Keane et al., 2009; Overbaugh and Schultz, 2015; Perkins, 2008; Starr, Manaris, and Stalvey, 2008).

3.4.1. Cognitive domain Bloom's taxonomy

One of the most popular and well-known models of cognitive human processes is Bloom's taxonomy. Originally established in the 1950s, Bloom's model remained unchanged until very recently (Sousa, 2006). The taxonomy was published in an updated edition by Anderson et al. in 2001. According to contemporary educational theory, this new taxonomy is appropriate (Sousa, 2006). The difficulty rises as the student moves through the six levels in each of the two versions of Bloom's taxonomy.

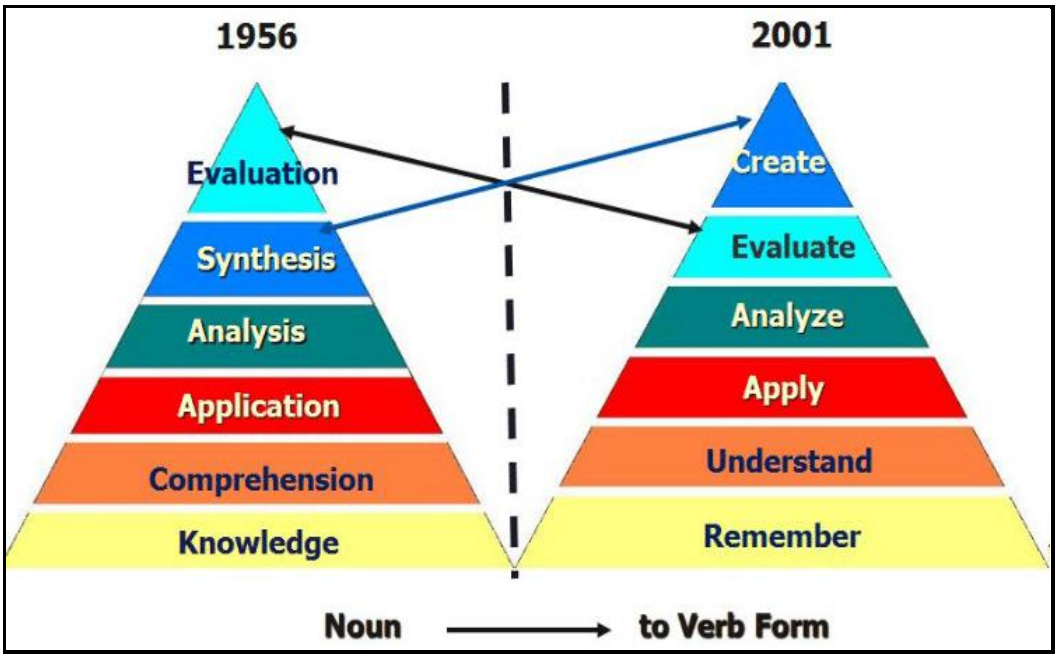

Figure 3.1: Original and Revised Blooms Taxonomy (Sousa,2006)

There are two main differences between the taxonomy's initial and revised incarnations. The new version also more properly describes each level's intended sense by using informative verbs for each level. Second, the final two phases of the first edition were changed in the revised one. Recent research has shown that making decisions based on predetermined criteria is easier than creating, planning, and producing an initial product (Sousa, 2006, p. 250). The hierarchy of complexity in the new taxonomy is consequently less linear than in the original since it recognizes that a person can move between the levels throughout extended cognitive activities.

The revised taxonomy edition is the focus of this study. In this thesis, wherever Bloom's taxonomy is mentioned, the updated version should be taken as intended unless otherwise noted. Each of the six steps of this updated taxonomy is briefly described below. (Sousa, 2006:250-252):

- **Remember**: Recall is the rote recall and identification of facts that have previously been learned. Because there is no assumption that the student understands what is being recalled, this level reflects the lowest degree of learning in the cognitive domain.
- **Understand:** The capacity to comprehend the material is described at this level. The learning here goes beyond mere memorization. If a learner comprehends the subject, they can utilize it to solve problems and make decisions in the future.
- **Apply:** The third level expands on the second by requiring less guidance when applying previously learned material in fresh contexts. This comprises using concepts, theories,

methods, and rules to address issues within the specified domain. This level combines the use of convergent thinking and procedural memory to choose the appropriate knowledge and apply it to a brand-new problem. To reach this degree of learning, practice is necessary.

- **Analyze:** This is the capacity to simplify difficult ideas in order to comprehend their structure. Understanding the basic components of a complicated system and exploring the connections between them and the whole are examples of analytical talents. Because the learner must be aware of the mental process being used and understand both the substance and the organization of the material, this stage is deemed to be more difficult than the third.
- **Evaluate:** Evaluation is the process of determining something's worth in light of predetermined standards and criteria. The student may choose these standards and/or criteria, or they may be assigned to the student. This is a high level of cognition since it calls for the integration of components from numerous different levels with conscious judgment based on predetermined standards. A pupil must develop their thinking in order to reach this level, and they should also be more open to different viewpoints.
- **Create**: The ability to combine different elements to create a new thought or plan is what is meant by this level, which is the highest in the taxonomy. This level emphasizes originality and the capacity to create novel structures or patterns through divergent thought.

To increase student success and set performance goals, educational taxonomies like Bloom's taxonomy are helpful tools (Fuller et al., 2007). The two popular taxonomies of education are both general. All disciplines with a hierarchy of learning outcomes are meant to be included in these taxonomies (Fuller et al., 2007). The Bloom taxonomy will thus apply equally to a more traditional subject, like zoology, when it comes to corporate information security education.

3.4.2. Education in cyber security using Bloom's taxonomy

Perceptual, emotional, and other phases at which the learner works are identified and categorized by the trainer using learning taxonomies. with general terms, it could be claimed that learning about taxonomies aids with interpretation (Fuller et al., 2007). This kind of meta-knowledge is typically lacking in training and safety teaching. Siponen (2000) explains awareness and education programmes widely in two sections, i.e., the structure and content. The Structure group covers problems that can be discussed structurally and quantitatively.

These problems are more explicit knowledge. However, the second group contains more implicit interdisciplinary awareness. Deficiencies in this second field typically invalidate systems of awareness (Siponen, 2000). For example, how to encourage users to stick to security standards is a matter that will be part of this type of content.

Consumers may purposefully ignore safety policies even if they are aware of them because they do not comprehend why they are necessary (Schlienger & Teufel, 2003). Understanding and inspiration both rise when the "why" question is addressed (Siponen, 2000). It would not be likely to improve morale or behaviour merely to remind the workers that "this is our strategy" or "you just need to do so," mostly as is common (Siponen, 2000). Breath-taking, active, mindful, and positive activity, driven by intentions and feelings, is learning (Garde et al., 2007). Many constructivist models of learning indicate that learning should be student-centred (Garde et al. 2007). Students must involve any individual in an organisational information management education campaign. It is also necessary to note that each student must excel in the campaign (Van Niekerk & Von Solms, 2004).

It is highly necessary to consider the learning needs of workers to ensure effective learning for all workers. Roper, Grau, and Fischer (2005) suggest that administrators frequently try not to fully research and consider the reasons behind these demands to meet the protective education needs of their workers. The best educational materials will be those that are specifically designed for the learning needs and learning preferences of the students (Van Niekerk & Von Solms, 2004; NIST 800-16, 1998). Another argument is that awareness campaigns that are not tailored to a target audience's specific hobbies or interests are unsuccessful. Recognizing these demands could be aided greatly by a learning taxonomy.

Before putting together, the educational campaign content type, information protection specialists might utilize a taxonomy, such Bloom's taxonomy. Such a taxonomy may make it easier to communicate the target group's learning requirements. It might also lessen the tendency to concentrate just on the framework used in these efforts. The level of Bloom's taxonomy will initially be recalled and likely understood by merely explaining what a password is. However, the amount of taxonomy evaluation knowledge needed to understand why their passwords are important, should be properly created, and saved could be just as high.. An information security specialist might think that simply explaining passwords to consumers is sufficient, but research has shown that employees' understanding of the importance of employee buy-in is crucial. According to Siponen (2000), Schlienger and Teufel (2003), Van Niekerk and Von Solms (2004), and Roper et al. (2005), this level of awareness inspires behavior change.

By incorporating an education taxonomy into the development of an information security curriculum program, the appropriate degree of learning in the cognitive domain may be ensured by comparing the curriculum's requirements for evaluation and content to the taxonomy. Based on an assessment of the interests and needs of the target population, a set of clearly stated success goals "should be the basis for any instructional plan" (Roper et al., 2005). The right use of instructional taxonomies not only aids in the expression of these achievement expectations but also aids educators in making accurate assessments of the population's needs and preferences. Table 3.1 provides an illustration of how Bloom's revised taxonomy might be applied in the context of information security.

Level	**Terms**	**Sample activities**
Create	Imagine Create a design Infer	- Act as though you are an information security officer for a major company. - Report on a recent security event in writing. Reporting an incident in the form of a news story. - Create a new policy provision to forbid users from storing confidential data on mobile devices. - Construct a hypothesis to account for the continued use of password writing by employees.
Evaluate	Appraise Analyze Judge Critique	- Which of these policy items would be more appropriate and why? - Is it reasonable to require employees to never use their work email for personal purposes? - "Why" or "Why not"? - Which of the security standards you have researched is more suited for usage in South Africa? - Justify your response. - Compare and contrast these two security products and explain why you would suggest one to a customer over the other.
Analyze	Compare, contrast, distinguish, and deduce	- Which of the following security breaches is most probable? - Compare and contrast the security requirements of manufacturing companies with those of banking organizations. - Sort these security measures in accordance with the broad principles they support. - Which of these practices might result from the specified policy?

Apply	Practice Determine Apply	- Use these mnemonic devices to help you remember and establish secure passwords. - Determine the level of security of the following password. - Consider three potential outcomes in the event that your password is stolen. - Please encrypt the following message using the provided tool.
Understand	Summarize Discuss Explain Outline	- Write a summary of the security policy provided in your - Why should a password contain characters other than - Describe the operation of symmetric encryption. - Describe your personal obligations in relation to the Write a summary of the security policy provided in your own words.
Remember	LabelRecall Recognize Define	- What constitutes a security incident? - Identify and label each threat in the image. - How does social engineering work? - Which image depicts someone shoulder surfing?

Table 3.1: Information Security according to Bloom's Taxonomy (Anderson et al., 2001)"[1]

This example is meant to serve as a starting point for ISOs looking to use Bloom's taxonomy to develop awareness and training campaigns rather than as a final statement. But it should be obvious that this taxonomy might be usefully applied to precisely classify the majority, if not all, educational information security needs. When grading in accordance with a taxonomy like Bloom's, it may also be simpler to find information on pedagogical strategies suitable for assisting students in achieving the required level of cognitive comprehension.

As was already noted, Bloom's taxonomy is further divided into four information groups and six cognitive domain levels. A series of statements outlining the academic objectives of an educational program with one or two of the four categories of information are often included with activities on the six cognitive stages. A statement of learning intent is typically used to create a number of learning assignments. Activities that support learning are known as learning activities. A learning activity is made up of a verb that describes a cognitive activity and a noun that adds more context to the relationship between the learning intention and a knowledge group (Anderson et al., 2001).

Learning taxonomies help educators characterize and organize the phases that people go through as they learn in terms of cognitive, affective, and other characteristics. To put it simply, comprehending taxonomies aids in our ability to "understand about understanding" (Anderson et al., 2001). Additionally lacking from this level of metacognition is end-user information security education. Siponen (2017) notes that knowledge and education programmes can be

commonly defined in two groups, namely structure and material. The Structure group covers problems that can be discussed structurally and quantitatively. This problem is more explicit information. However, the second group contains more implicit interdisciplinary awareness. Deficiencies in this second sector typically invalidate systems of understanding (Siponen, 2017). For example, how to encourage users to stick to security standards is a matter that will be part of this type of material.

It is highly necessary to consider the learning needs of workers to promote effective learning for all workers. Managers frequently aim to fix workforce safety communication needs without fully researching and recognizing the causes of driving them (Bartholomew, 2015). The claim was made earlier that curriculum materials should be adapted to specific learners' instructional conditions and styles (Bialaszewski, 2015). One may also claim that awareness initiatives that were not suited to individual preferences or the interests of a defined audience community will not succeed. A taxonomy of learning may play an important role in recognizing these needs (Cheung, Cohen & Elia, 2011). Specialists in the computer technology area can use a taxonomy, including the taxonomy of Bloom, before assembling the educational campaign type.

Such a taxonomy may make it easier to communicate the target group's learning requirements. It might also lessen the tendency to focus primarily on the structure of these efforts. For instance, to teach a human what a password is, one must remember and possibly comprehend the level(s) of Bloom's taxonomy. The amount of information needed to understand why your passwords are important and should be carefully created and saved, however, might equal the taxonomic evaluation criteria. An information security specialist could think that simply explaining passwords to users is sufficient, but research has shown that it is crucial to consider the reasons why employees need to buy-in. Improvements in behavior are motivated by this level of awareness (Cheung, Cohen, & Elia, 2011).

3.5. Conclusion

The theoretical basis indicates that the education curriculum for information management would be more successful if it adopted pedagogical standards. It has been made clear that it is not preferable to classify security education requirements according to wide knowledge, preparation, and educational classifications. Rather than using an instructional taxonomy, such as the Bloom taxonomy, the security education needs of corporate users should be specifically specified. By using this taxonomy, some common vulnerabilities may be resolved in ongoing security knowledge and education programmes.

An explanation of how the taxonomy of Bloom could be extended to the security definition of knowledge was presented. The main flaw in this research is the dearth of evidence supporting the taxonomy of Bloom's proposed application. Future research in this area should focus on overcoming this weakness. It has previously been recommended that security professionals studying or practicing human science should "borrow" when necessary, from the humanities rather than re-inventing the wheel.

CHAPTER 4

RESEARCH METHODOLOGY

4.1. Introduction

Both study and common sense include an effort to comprehend diverse facets of the world. Research is an explicit, systematic approach to learning, frequently through a process of checking beliefs, although perhaps not common sense (Berg 2007:12). The selection of a research question is the first step in this procedure. Once the study question had been established, it was required to conduct a literature evaluation and select a research design. At this phase, choices were made regarding the types of data to be gathered, the methods to be used to gather them, the respondents to be invited, and the methods to be used to analyze the data.

The research technique and step-by-step instructions for this study are covered in this chapter. Discussions also include participation selection, participant profile, and access to organizations and people. The respondents' ethical and secrecy commitments made at induction are also included in this chapter. Additionally highlighted are the approaches employed for data collection, interpretation, and analysis, as well as the reliability metrics applied.

4.2.Research methodology

The study adopted Design-based research (DBR), which is iterative, integrating, flexible, context-based, pragmatic, and grounded in both theory and real-world contextual situations. DBR is described as "a series of approaches, with the intent of producing new theories, artifacts, and practices that account for and potentially impact learning and teaching in naturalistic settings," according to Barab and Squire (2004: page 2). This research approach possesses all the traits that enable organizations to produce the required research results. DBR is appropriate since it provides a chance to examine the research goals in relation to the theoretical framework and research paradigm. The researcher intended to do a study of the relevant literature to choose the topic, then collect data using the various research methods listed below, analyze the data, and utilize the analysis to guide the design of the intervention. The intervention, in this case, are in the form of cyber security curriculum framework. The research outcomes can only be achieved by interacting with various role players in our education system.

The study explores existing interventions to further Cyber security education in South Africa in a mixed research design approach that considers both the qualitative and quantitative content available.

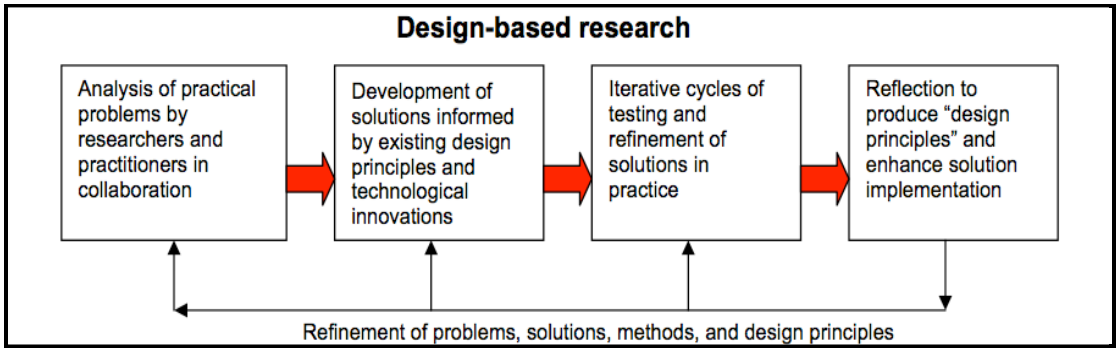

Figure 4.1: Design-Based Research (Amiel & Reeves, 2008)

4.3. Research Approaches

This study is centred around two aspects. The primary one is comprehending how cyber security courses are instructed and controlled. The second is to devise an extensible structure for cyber security courses that could streamline any difficulties dependent on the consequences of the principal question. This implies this proposal is partitioned into two sections, each requiring diverse techniques.

The methodology for this study is a mixed research design approach. For the principal objective, a mixed methodology appeared well and good depending on the way that the examination question is centred around a "scan for understanding, a portrayal of things happening pretty much in the meantime without desire or causal clarification" (Kvale, & Brinkmann, 2009:38). Nevertheless, assessing the curriculum requires an alternate strategy. To structure a product design, a strategy for assessing programming engineering is required.

The researcher's ontological leanings are clearly toward a form of critical realism, where the actors (in this case, managers in HEIs) work within limitations imposed by society and a variety of other relevant dynamic organizations (Leedy & Ormrod, 2010). This is evident from the provided assumptions and interpretations throughout the literature review. In light of this, the research takes a pragmatist stance that lies somewhere between scientific positivism and the phenomenological or interpretive approach common in qualitative studies. Due to the organizational structure of the study, it is challenging to gather the necessary value-free data for a positivist investigation (Robson, 2012). Rather, the respondents' perspectives and understandings of organizational realities are embraced for what they are. Each actor interprets organizational facts and their place within the institution differently. However, for each of

them, fulfilling some administrative objectives as well as some intellectual and academic objectives is likely to be necessary for organizational success.

According to Remenyi, Williams, Money, and Swartz (2005), a critical realist research technique admits that social constructionists' views play a significant part in constructing reality and holds that any investigation should begin with the actors' perceptions (Archer 1998). Critical realism is referred to as "a particularly appropriate framework for designing real-world studies" by Robson (2012, page 17). The author presents a strategy that can provide the advantages of a systematic approach and acknowledges the existence of reality (realism), while at the same time maintaining a sceptic attitude and allows for the major change of realities by the perceptions of the actors. The strategy encourages proper concept inspection, debunking, and an ethically sound method of conducting research in an organizational setting.

In addition, the direction of this research is relevant to the assumptions about the nature of knowledge made by Corbin and Strauss (2008: page 8).:

> *"Any approach that attempts to comprehend and explain occurrences will need to be complex since the world is exceedingly complex and there are no simple explanations. Instead, events are the product of numerous forces combining and interacting in complex and frequently unexpected ways."*

Corbin and Strauss (2008) point out that reality is not constant and is subject to interpretation in rejecting a positivist approach. They also challenge a completely constructivist point of view by arguing that the researcher must comprehend and accept some outside factors.

The research orientation in the study is situated between positivism and an interpretive approach based on a quantitative and qualitative case study (Yin, 2009; Robson, 2012) and supplemented by a thematic review because of the researcher's philosophical position and the assumptions and interpretations stated above. A variety of viewpoints indicative of a relativist perspective were expected to be revealed by the interviews performed as part of the data collection procedure.The research perspective is not fully inductive in approach because it also draws from exposure to a variety of sources. Prior to comparing these results with best practice measures drawn from the literature of Cyber security curriculum, the emphasis is on the practical, trying to ascertain what works and what is less successful in the researched institution (UNISA).

4.3.1 Appropriateness of Mixed Research Design Method

Adopting a mixed research design method, mixing design based research and case study approach is superior to a single method as it is likely to provide rich insights into the research phenomena that cannot be fully understood by using only qualitative or quantitative methods however using both methods will ensure that qualitative and quantitative data are simultaneously collected, analyzed and interpreted for a complicated research that requires breadth and depth of the subject to be explored. The use of mixed research design method enables the research to answer research questions with sufficient depth and breadth (Enosh, Tzafrir, & Stolovy, 2014)

Collecting data from multiple sources can also augment validity and reliability of the data interpretation. A mixed research design can integrate and synergize multiple data sources which can assist to study complex problems (Poth & Munce, 2020). Use of qualitative research tools like interviews will allow this research to triangulate quantitative data for well validated conclusions.

For this research it was natural choice to adopt a real-life case, through mixed research design method, of MICT SETA in analysing the complex cyber security training environment. This offers a logical ground, methodological flexibility, and an in-depth understanding of smaller case like the SETA (Maxwell, 2016). Design based research will allow this research to collect the data from many participants; thus, increasing the possibility to generalise the findings to a wider population whilst the case study approach on the other hand provides a deeper understanding of the issue being investigated, honouring the voices of respondents. It also allows the researcher to widen the exploration, enquiry and investigation since quantitative data bring breadth to the study and qualitative data provides depth to it. Moreover, quantitative results can be triangulated with qualitative findings as noted above. This is a clear opportunity to answer research questions by combining two sets of strengths while compensating at the same time for the weaknesses of each method (Johnson & Onwuegbuzie, 2004).

4.4. The Research Sample

Curriculum development managers and lecturers (STEM) from MICT SETA were contacted to participate in the study, which used a case study methodology (Maxwell, 2012). A wide spectrum of expertise and participation in the subject of cyber security were tapped through the

questionnaire and interviews. Most significantly, they are required to discuss their involvement in teaching IT and delivering other cyber security programs to South African students. MICT SETA was chosen for this study because, in comparison to other schools, it has a high-profile international student population and has evidence of the mounting pressure to handle cyber security. The fact that MICT SETA accurately represents the range of and geographic location encountered throughout South Africa's education sector was the second most important factor in developing the case study.

This study will employ the Merriam and Tisdell (2015) method of purposeful sampling. Additionally, MICT SETA employs personnel who have been engaged in the community and are generally familiar with those who are leading the development of pertinent initiatives in the nation. This strategy will be intended to lessen the possibility of a negative reaction (Lewis, 2015). After receiving approval to conduct the research, invited respondents were sent an email with a brief description of the project's goals, their specific responsibilities, and an overview of the anticipated advantages for the institution. This method of access was considered morally sound. The project team and project managers communicated with one another via email. This was not only a fundamental but also cost-effective strategy because it was seen to be the most equal in preventing any bias against the respondents as well as the institution.

Non-probability convenience sampling was also used by the researcher (Creswell, 2013). A non-probability sampling technique called convenience sampling involves taking samples when it is most convenient for the researcher. According to Hair, Black, Babin, Anderson, and Tatham (2006), the target population was assumed to be homogeneous, and the individuals chosen to represent the target population as a whole with regard to the features of the organizations under study. The cover letter included a standard set of instructions that explained the goal of the study, how to reply to the questions, and encouraged responders to participate in the study.

The researcher thought that by choosing this institution as the case study, some of the institutional characteristics that would normally obstruct the analysis of the development and teaching of cyber curricular materials would be eliminated (Bourne, 2014). The location selection was made in the hopes that it would present certain opportunities and insights into staff behavior that would not have been detected if a different institution or institutions had been selected. Even though it would have been beneficial to have additional case studies, it became necessary to stick with one institution after persistent lobbying and interaction with

several institutions. This choice was partly influenced by the difficulty encountered in gaining access to other institutions. In terms of sample techniques, this study used random sampling for the unknown population of scholars and non-random sampling for the known population of education authorities. The sample design was stratified sampling, with the following categories further divided into smaller groups: lecturers, the department of curriculum development, cyber security, and educators.

4.5. Data Collection

For qualitative research, this study used interviews to collect meaningful content, a survey questionnaire with randomly sampled research respondents and online surveys for purposefully sampled respondents for quantitative triangulation of data i.e., Information and Communication Technology (ICT) professionals and ODL curriculum designers.

4.6. Data analysis

Data obtained was then analysed concerning research questions as stipulated above. This entailed descriptive analysis whereby trends in the offering of cyber security content are analysed. Condensing the information that has been acquired and presenting the findings in a way that communicates the most important elements are both parts of the data analysis process throughout a research project. The researcher used a variety of techniques to establish the most thorough perspective possible during the data analysis for this investigation. Different approaches call for different kinds of research. The study utilized components of constant analysis in terms of the initial content (Creswell, 2014).

Creswell (2017) went on to explain that there are two levels at which the data collected can be analyzed. The most fundamental level of analysis deals with what was said, reported, or observed without any expectations or further interpretation. It also comprises the most distinct study of the information. This is referred to as the display level of investigation in some of the literature. The second level focuses on the interpretative examination of the data and examines any hints or conclusions that could have been drawn from the response, the information gathered, or the inferences made. The qualitative interview transcripts can provide a lot of information. This is expected to be the most extreme and important component of the investigation and will be sorted or generally translated significantly.

According to Kvale and Brinkmann (2009), the content body should analyze the information gleaned from the voice group's focus group and interview data. This was accomplished by using a seasoned transcriber's skills. The purpose of the content analysis process will be to identify the major themes and topics that emerge from the interview transcripts (Maxwell, 2005).

Computer-assisted qualitative data analysis programming (CAQDAS-Nvivo adaptation 11), according to Wiedemann (2013), is useful for coding information, breaking it down into manageable pieces, and differentiating or labeling these fragments. Throughout the process, it is possible to successfully code, record, or modify new concepts, categories, and subjects.

The qualitative data were organized using Nvivo version 11. With the help of the program Nvivo, a sizable amount of qualitative data is grouped and reduced to a manageable volume. The following steps are included in the data analysis:

- Establish multiple codes as the first step.

- Using the coding created in step one, reduce the data in step two. To make the analysis easier to understand, comments will be included in addition to the codes.

- The system will create a coding plan diagram that recognizes and labels the codes as well as the relationships among the codes as third step

- As a last step the code chief window will generate a table of code numbers, which will be stored as an archived document or an Excel record.

A hybrid coding approach was used for the coding, combining codes from the master reports' records with those from earlier open coding. The researcher will code the data that will be gathered from the field and the itemized transcripts made as long as valid data to refine codes using the codes that will emerge from the preliminary round of open coding.

According to implications that the researcher identified in the data, sections in the information are coded (Brechbhl, Bruce, Dynes & Johnson, 2010). The interviewer writes down the coding's key points. Another researcher was given a sample of the transcripts to cross-code for validity. A strategy will be created to organize or accommodate the coding variations between the researchers with the end goal of reaching consensus in the coding.

In addition, until the respondents reached a state of immersion, the researcher read the data transcripts numerous times (Maxwell, 2005). The themes were then put together into more logical groups, and a list of the main themes that emerged from the respondents' responses will be created (Thorpe & Holt, 2008). Following that, these themes will be used to infer conclusions and recommendations.

Due to the nature of this study, a statistical analysis program known as SPSS version 12 was utilized for quantitative data analysis, which involved statistics and graphic representation (George & Mallery, 2013). Phase one of the data collection procedure includes information gathering utilizing closed-ended questions to ensure adequate triangulation of findings. This required that most of the open-ended questions be coded and turned into numerical data. The verbal and visual information gathered from the interviews and observations was then organized numerically to achieve this. The SPSS application was then used to analyze the same data. The translation of the open-ended questions into quantitative data was done with the researcher's goal of maintaining and preserving the qualitative meaning in mind (Sandelowski, 2000). As a result, only numerical items are functional in quantitative research. Data from quantitative to qualitative research were converted using the same procedure as data from qualitative to quantitative research. During the data analysis, it was decided whether to go from quantitative to qualitative study. To confirm that the information captured accurately reflected what the respondents had to say, the adjustments made were corrected during a follow-up session with the respondents.

4.7. Validity & Reliability

This study verifies whether the research outcomes are reproducible through internal validation whereby the data researched is compared to research questions and external validation to ensure that research conclusions are congruent with the state of Cyber security education amongst researched population groups.

Reliability refers to something that is dependable and will give the same results over time. The data in qualitative research is in a narrative form and subjective, thus making it difficult to obtain similar results. However, Zohrabi (2013) suggested overlooking the issue of the same results and advised considering the dependability and consistency of the data, thus implying that the researcher should collect data until the data collected becomes redundant. Three techniques have been used to ensure the dependability of the results.

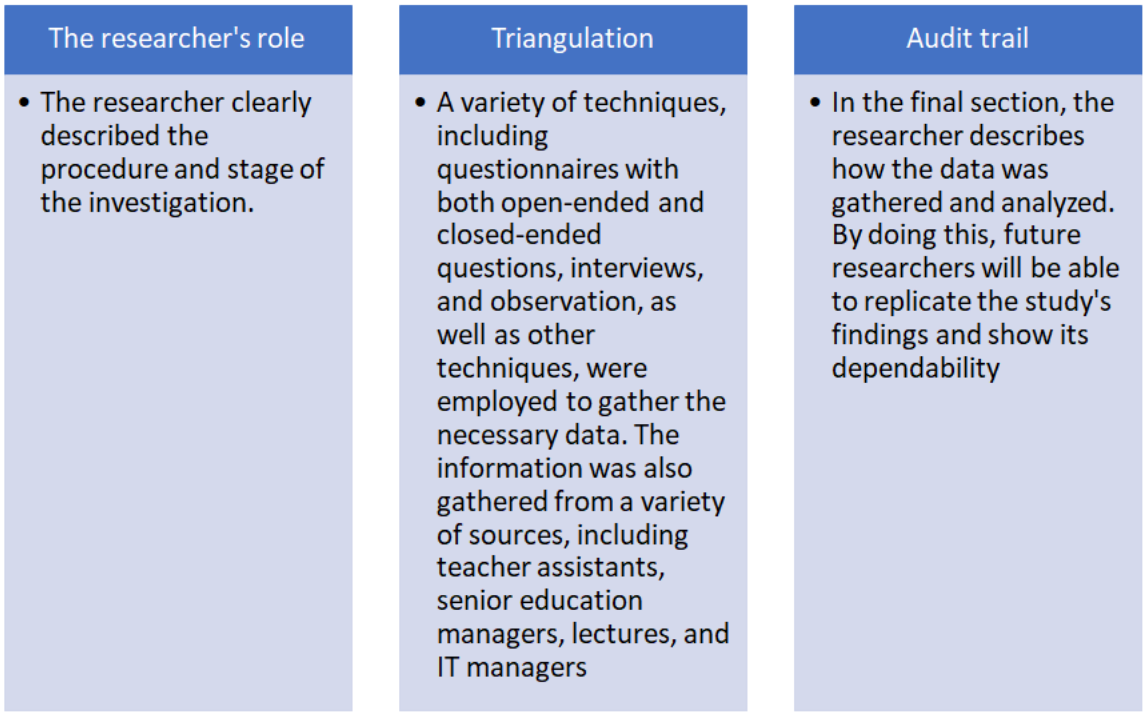

Figure 4.2 Results testing techniques (Zohrabi, 2013: 260).

Validity generally refers to making sure that a research study is both accurate and credible. As Joppe (2000:71) points out, validity governs whether the study measures what it was intended to assess or how accurate the study's findings are. Do you have the ability to hit "the bull's eye" of the study object with the research equipment, to use another phrase? To evaluate validity, researchers typically pose a number of questions, and they frequently resort to the work of others for a response.

In general, validity is about looking at the quality and the acceptability of the research. Validity requires that the instruments used are validated as the results or conclusions emanate from both the data and the instruments used (Zohrabi, 2013). Six techniques have been suggested by Zohrabi (2013: 252) as tools to ensure validity:

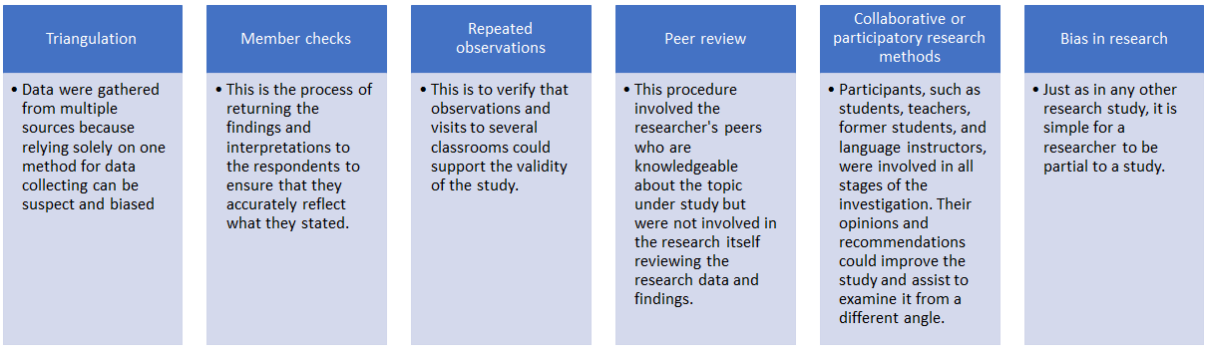

Figure 4.3 Techniques for validating instruments

As mentioned above, a good researcher collects data and analyses and interprets it without being biased. In addition, such a researcher observes all the ethical considerations of research. The researcher should always try to be non-judgemental and, as already stated, adhere to all the ethical considerations mentioned by Zohrabi (2013). All the above-mentioned techniques helped to ensure that the research is as valid and reliable as possible. They were taken into consideration by the researcher with most of the above-mentioned techniques of questionnaires, interviews and observations being used to avoid unreliable and invalid results.

4.8. Ethical Considerations

Research of this nature will involve engaging with scholars and complying with each individual institutional policy. This is undoubtedly considered in the study. To prevent the respondents in this research study from feeling burdened by their participation in the study, the researcher used different volunteers in the various phases of the investigation. The researcher adhered to the notion of voluntary involvement from the very beginning of the investigation. In other words, the research respondents were not forced to participate (Creswell, 2013). The fundamental ethical rules that must be followed when conducting research with people are respect, anonymity, beneficence, and fairness, as shown by earlier studies on ethical difficulties. Respect is defined as having enough regard for study respondents to inform them of the study's purpose and provide them the freedom to select whether or not they want to participate. The researcher must adhere to ethical norms by protecting the subjects from situations that could be physically or mentally harmful.

Research must also take ethical considerations into account in order to avoid any wrongdoing, such as dishonest behavior that disregards non-revelatory assertions, violating participant confidentiality, falsifying reports, deceiving people, altering receipts, dodging legal obligations, etc. (Cooper & Schindler, 2008). The following moral principles were upheld in this study:

• Scientific legitimacy: The study's scholarly integrity and exploratory credibility were guaranteed by the manner in which it was carried out. Unreliable practices, including the avoidance of unoriginality, are examples.

• Participation: Participants' secret was preserved, and their privacy was respected. Any information gleaned from the respondents' involvement in the study was kept private.

• Requests for authorization were handled properly - see the letters of confirmation and access included in the appendices.

4.9. Conclusion

The mixed research paradigm methodology covered in this chapter was used for the investigation. Purposive sampling and the domains of exploratory, descriptive, inductive research were developed. The study's research design and ethical issues were discussed. The procedures for data collecting, data analysis, and data interpretation utilizing the content analysis method were described. Tests for credibility, dependability, and triangulation were used to establish the validity and reliability (a measure of trustworthiness). The following chapter covers how the empirical study's data were presented, analyzed, and interpreted.

CHAPTER 5

DATA ANALYSIS AND INTERPRETATION

5.1. Introduction

The research's results are described and summarized in this section. A list of respondents has been provided due to ethical considerations, but identity has been preserved. The comments of their respondents have not been changed in any way to maintain their originality. Transcription and content analysis were used to interpret the data. Following interpretation, the data were analyzed to pinpoint important themes and subjects utilizing the input of the initial information generated by the qualitative data analysis application Nvivo. The specifics and summaries of the most pertinent data outputs are provided in the appendices at the conclusion of this study.

5.2. Quantitative findings

The analysis subsection covers key points of the results of the survey, such as details about respondents, cyber security skills demand in South Africa, opportunities for joint efforts to support the development of the cyber security curriculum and the conclusion.

5.2.1. Classification of Respondents.

To start from response rate, overall, about 70 emails were sent out and 30 responses were received: 22 out of the 30 respondents were males. Their ages fell within the range of 20 and 54. While the overall number of respondents is not very high, it is believed they reflect the situation and requirements in South Africa, more so that study was undertaken under very strict guidelines of COVID 19.

Regarding respondents' experiences in IT field, it varied from 1 year to more than 25 years. 10 respondents had more than 5 years of experience in IT field, 10 of them with more than 5 years in the same company or education institution; 6 had been employed in IT field for more than 10 years, 4 of them in the same education institution and company with more than 10 years of experience (more details are available in Figure 5.1).

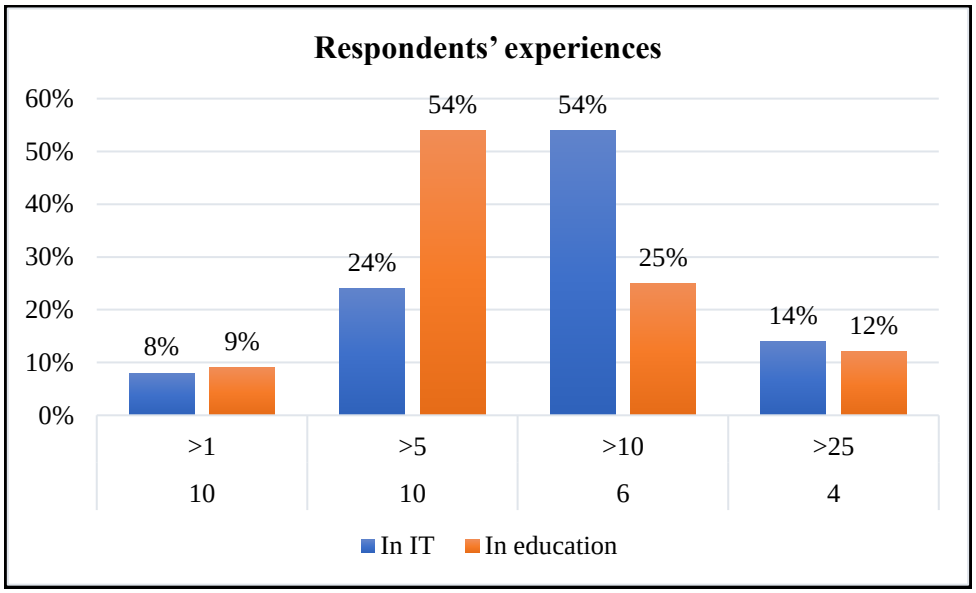

Figure 5.1. Years of experience of respondents.

Both management and non-management job titles were represented among the respondents' job positions. The Table 5.1 contains a detailed list. Listed under "Other" were the following occupations: program analyst, computer security expert, and deputy director of the IT field.

Respondents' positions	**Respondents**
Executive / C-level	2
Director	2
Manager	3
System administrator	5
Network administrator	3
Technician	7
Lecturer, Researcher	5
Security analyst	3
Developer	4
TOTAL	**30**

Table 5.1. Respondents' job titles.

The majority of respondents (both academic and non-academic personnel) worked for educational institutions (see Table 5.2). Four of the respondents were from sectors other than listed in the questionnaire: one of them represented Human Rights, one-Non-Governmental Organisation (NGO) and two were from a field of Trade.

Sectors	Number of respondents
Education	15
Technology & software	9
Banking/Finance	7
Communications	5
Health & social services	1
Energy & utilities	1
Transportation	1
Entertainment & media	1
Total	**30**

Table 5.2. Respondent breakdown by industry.

The primary focus of the study was MICT SETA as an organization that regulates the education industry, as was noted in section 4.4 of this thesis. In choosing which organization would be the focus of the case study, the 15 respondents from MICT SETA illustrate the range of profiles and geographic locations that are present within the South African education sector. However, to increase the study's scope for validity and dependability, other pertinent institutions, as seen above, had been approached.

5.2.2. Demand for Cybersecurity Skills

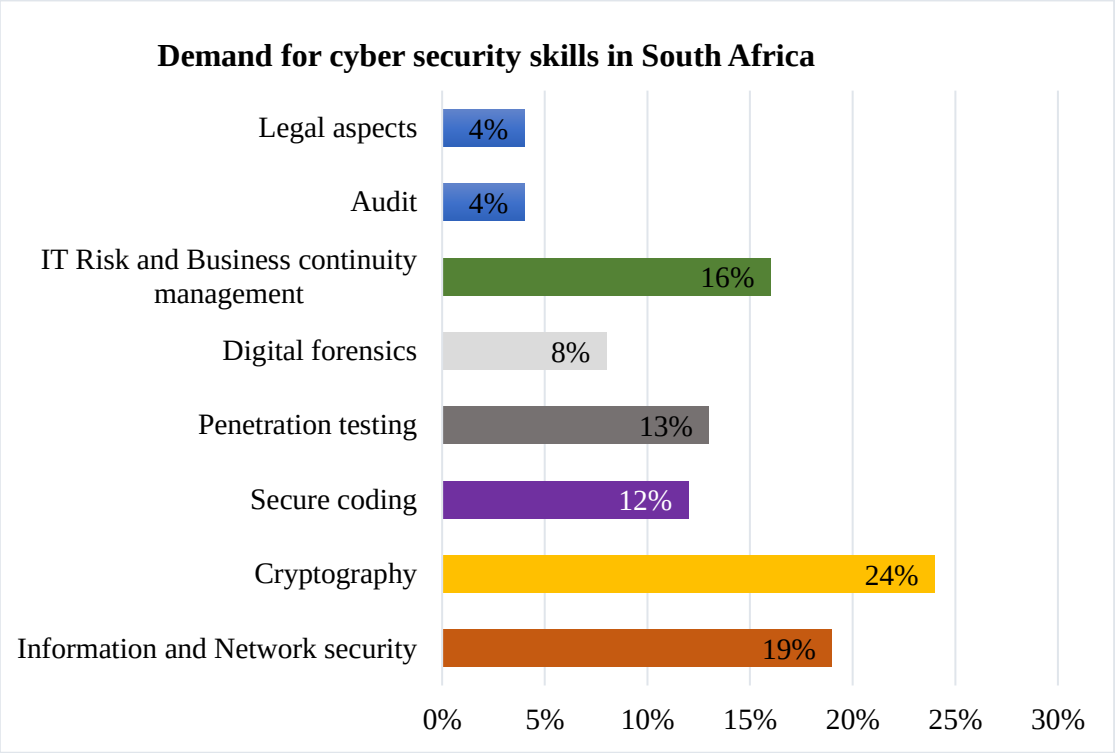

Figure 5.2. Cyber security skills in high demand in South Africa

t has been intriguing to start getting questions about how many companies have cyber security specialists. The findings indicated that the majority of the organization had little or no cyber security specialists. Out of 30 respondents, 22 said that the proportion of cyber security experts at their company ranged from 0% to 1%. Only one respondent (see Figure 5.2) acknowledged that the percentage at the company is 90%. Regarding forecasts for the future, it is important to note that most respondents (27 out of 30) anticipate a growth in the number in the upcoming 2-4 years.

5.2.3. Forecasted Cyber security skills in high demand in the next 3-5 years

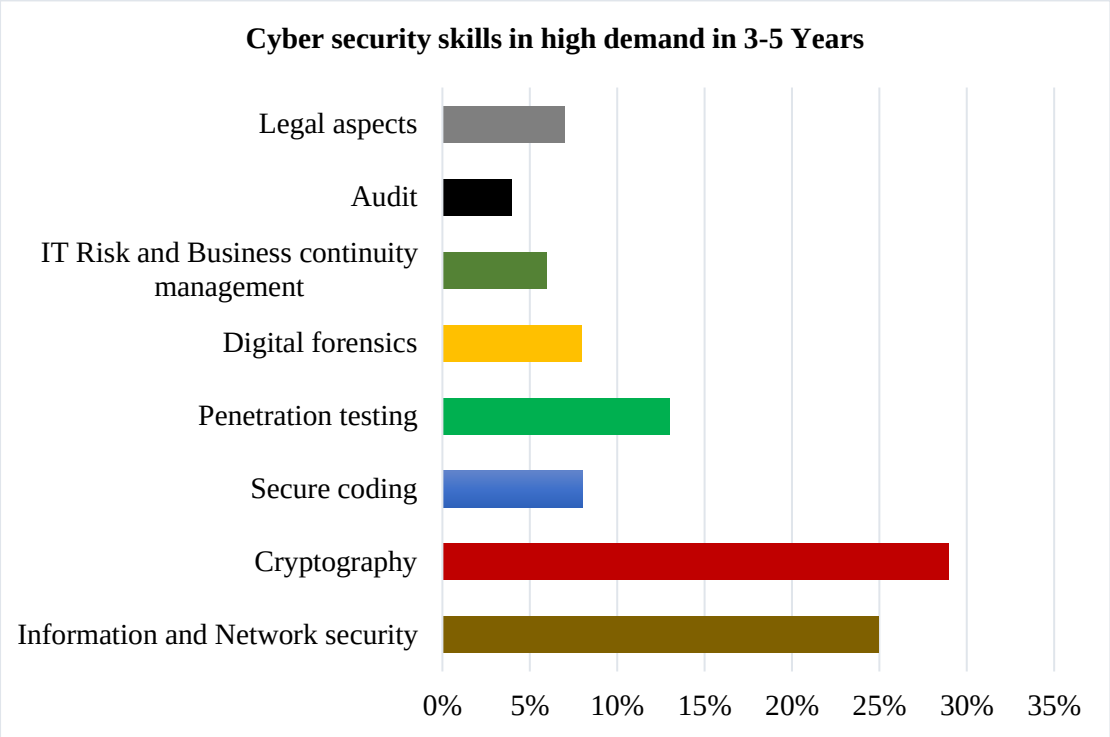

Figure 5.3. Cyber security skills in high demand in 3-5 Years

The respondents were asked which cyber security skills were important at present and which ones they expected to be important in the future, in 3-5 years. According to the results, currently the top five, the most demanding skills are: network security, cryptography, and penetration testing. Others are business continuity management, secure coding, and audit. The respondents predict that demand for secure coding and digital forensics will significantly expand in the future. The order of upcoming cyber security skills in demand looks as follows according to the results: network security maintains the lead position, next come Penetration testing, Business continuity management and Security coding with nearly the same score respondents, followed by audit, cryptography, legal aspects.

5.2.4. Cyber security professionals / skills that are difficult to find in South Africa at the present time

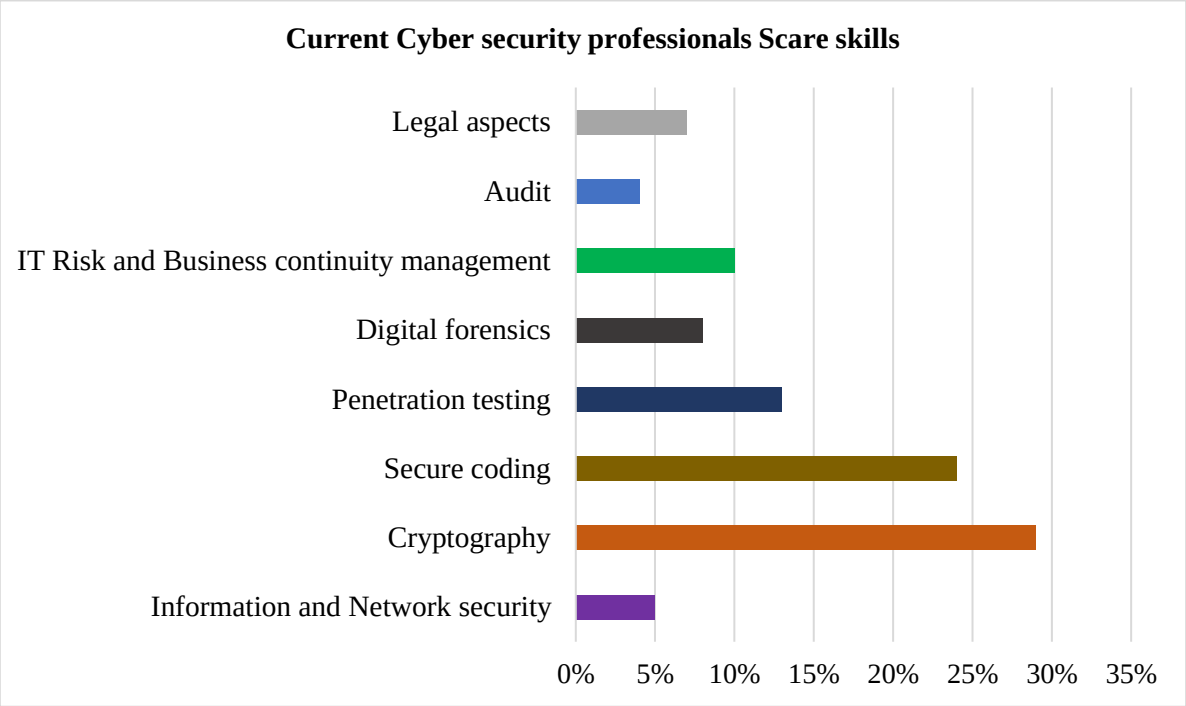

Figure 5.4. Current Cyber security professionals Scare skills

In comparison to the Figure 5.3 above the following Figure 5.4 below depicts cyber security skills demand now and in 3-5 years in South Africa, according to the respondents. These are Cyber security course taught education institution. The findings show that coding and cryptography are critical scarce skills whereas coding and BCM, appear to be most addressed programmes in most training institutions.

Both groups of respondents were asked, professionals with which cyber security skills were difficult to find in South Africa and which cyber security skills were difficult to recruit in South Africa. The combined responses show that the most difficult to find is a professional with cryptographic skills, next come digital forensics, secure coding, penetration testing, business continuity management (BCM), network security, legal aspects, audit, and reverse engineering. Regarding difficulties in recruiting cyber security skills, the most scarce appears to be recruiting in digital forensics, followed by penetration testing, secure coding, cryptography and BCM, less rare - network security, legal aspects, and audit. Reverse engineering was added by two respondents to the list of talents.

5.2.5. Cyber security course taught education institution

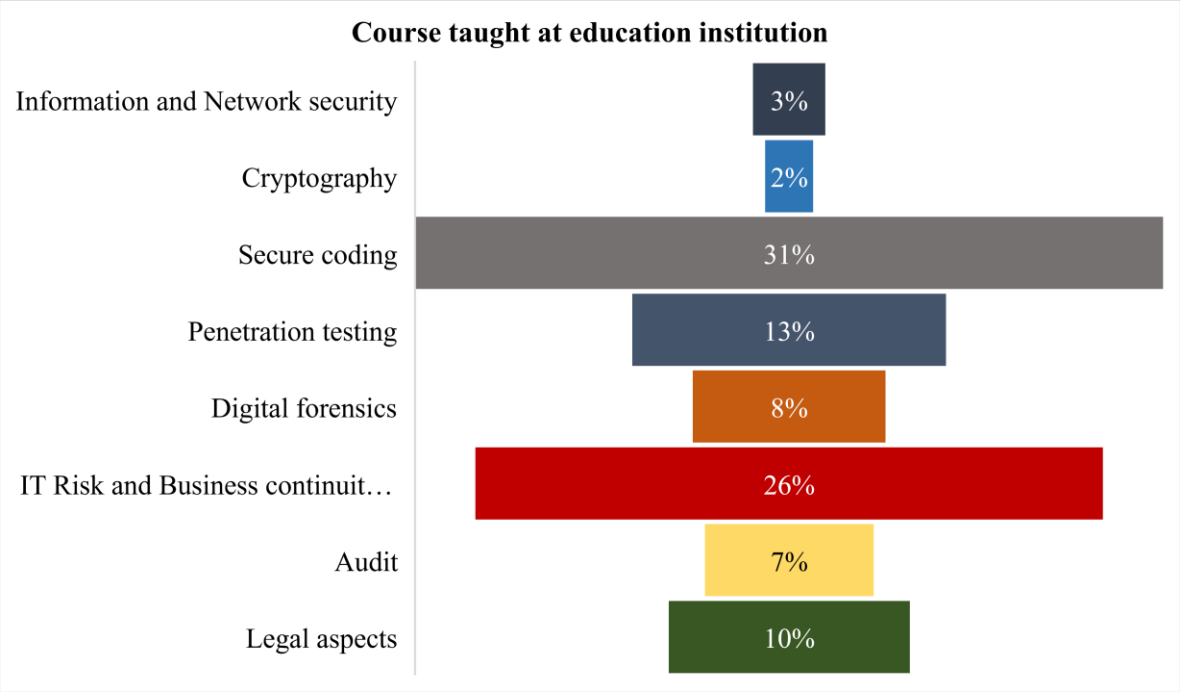

Figure 5.5. Common Courses Offered at Educational Facilities

The acceptance of the majority of cyber security programs has been disappointing when considering the responses, with the exception of codding, which may have been greatly influenced by country-specific 4IR framework, and the standard risk and business continuity management course. Referring to the finding by Renaud et al. (2018), it should be noted that the teaching of cyber security in higher education predates these initiatives and that there has been acknowledgement of the necessity for its inclusion as a subfield of computer science for a number of years. The definition of curriculum to enable this, which added "Information Assurance and Security" for the first time and for specialized cyber security degree programs, has been the subject of numerous worldwide and nation-specific initiatives.

The disappointing conclusion from the responses is that future generations of South Africans will be more vulnerable to cyber-attacks because they will have insufficient awareness of privacy and security issues if they do not study CS. And, unfortunately, women will bear the brunt of the consequences. The South African government must do more to educate its citizens about the importance of cyber security; universities alone can no longer shoulder this responsibility. It is imperative that all students, regardless of gender, receive an education in basic cyber security skills beginning in elementary school. There is too much at stake for any government to leave cyber security education and preparedness up to chance.

5.2.6. Options for education in cyber security today and in the future.

To investigate the demand for education in cyber security from companies now and in the next five years based on the responses of the respondents: in response to the question which requires the companies to consider improving the cyber security qualification of their employees now, most of them responded that it is not considered at all. To investigate the demand for education in cyber security from companies now and in the next five years, click here. There are only a handful of people in South Africa who are contemplating receiving training from organizations outside of their companies, receiving training in another country, or receiving training from their own companies. Fewer people are thinking about pursuing higher education. Only two of the respondents mentioned "self-education" as a potential additional choice. It is predicted that more responders than at the moment will be thinking about going to college between 2022 and 2027. The majority of them plan to take part in international and external trainings.

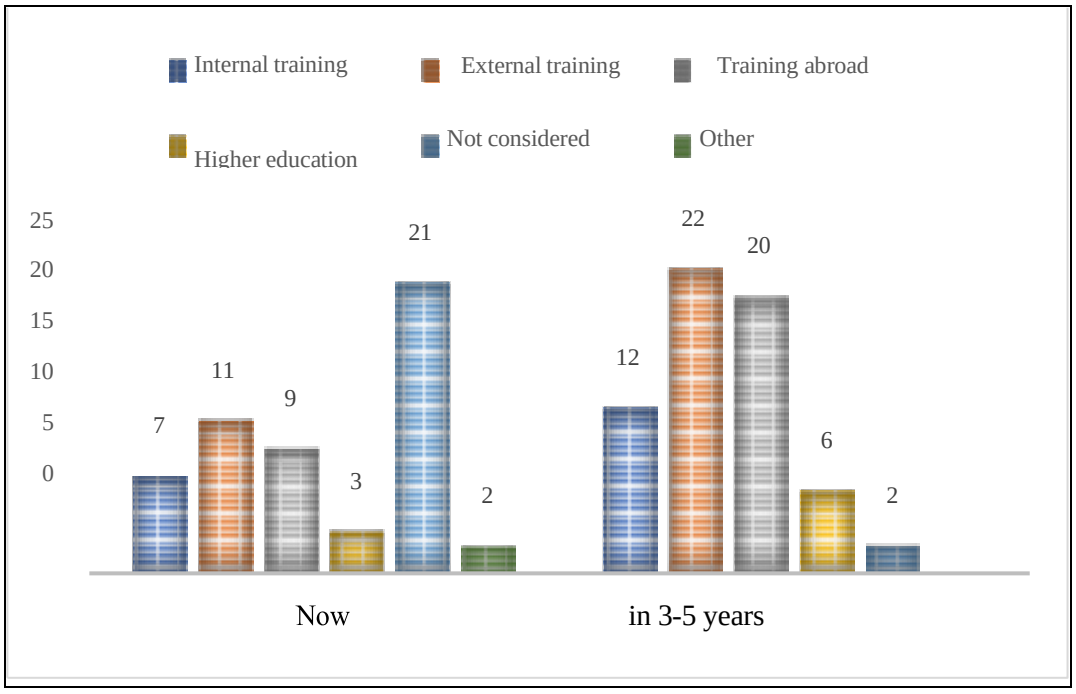

Figure 5.6. Options for education in cyber security today and in the future.

Many of them look forward to taking part in international and external trainings. Of the 30 respondents, 26 replied "no," 7 said "yes," and 6 stated that they had no knowledge of whether their company had contacted educational institutions. When asked whether any businesses had reached out to them to request cyber security training to increase the qualifications of their staff, 3 out of 7 responded positively, t3responded negatively, and 1 did not respond at all. The responses to the question of whether businesses are interested in cyber security graduate

programmes were broken down as follows. 2 faculty members have come forward to say that business interests have been taken. There was no such case, as 4 of them noted.

5.2.7. Cyber security programme multidisciplinary approach

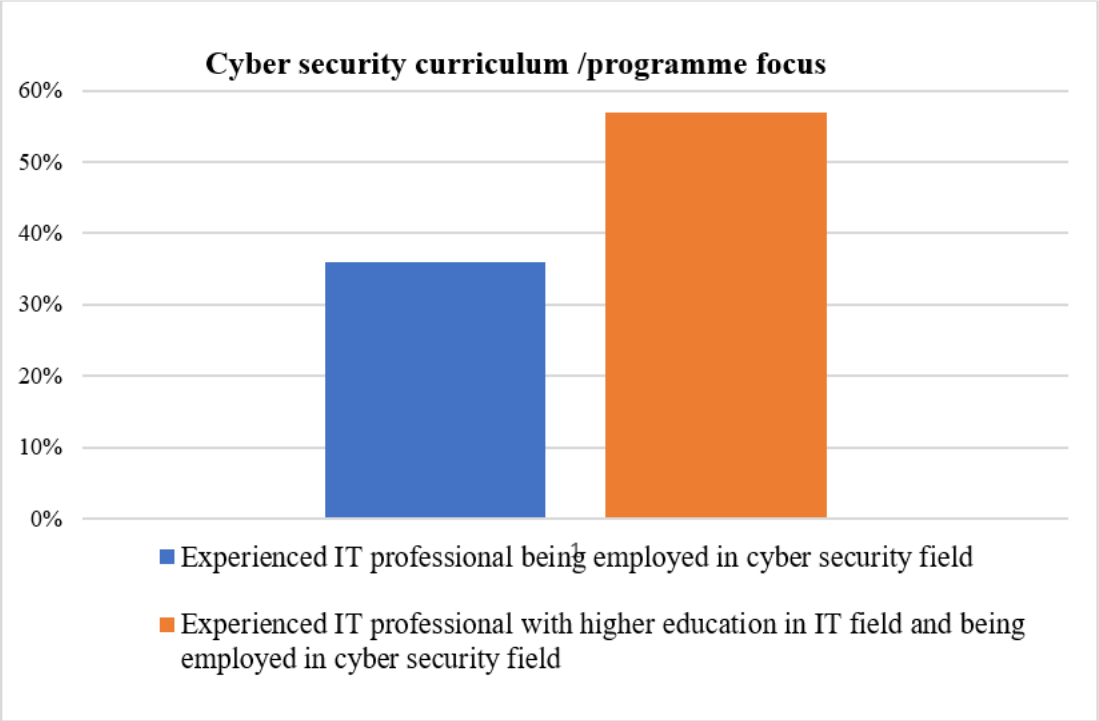

Figure 5.7. Cyber security curriculum /programme focus

Much as most participant indicted that such curriculum programme should be handled by IT professionals in the field of cyber security, all agree towards a multidisciplinary approach that is better than a narrowly focused. When asked which cyber security skills the programme should prioritise, businesses and educational institutions have offered slightly different recommendations, but the top five have remained consistent across the board. Cryptanalysis, Cyber security, code protection, and digital forensics as shown in the figure below.

5.2.8. The cyber curriculum or programme focus

The development of these programs should consider the objectives of the alumni, whether they are employed in government, industry, or academia. Several responses point to re-arranging the curriculum so that students take classes from a wider variety of disciplines and develop a broader range of skills. If the goal of the degree is to prepare students for work in the industry, then the curriculum should emphasise technical and hands-on skill development. On the other

hand, if the goal is to prepare students for graduate study and research, then the curriculum should emphasise conceptual development.

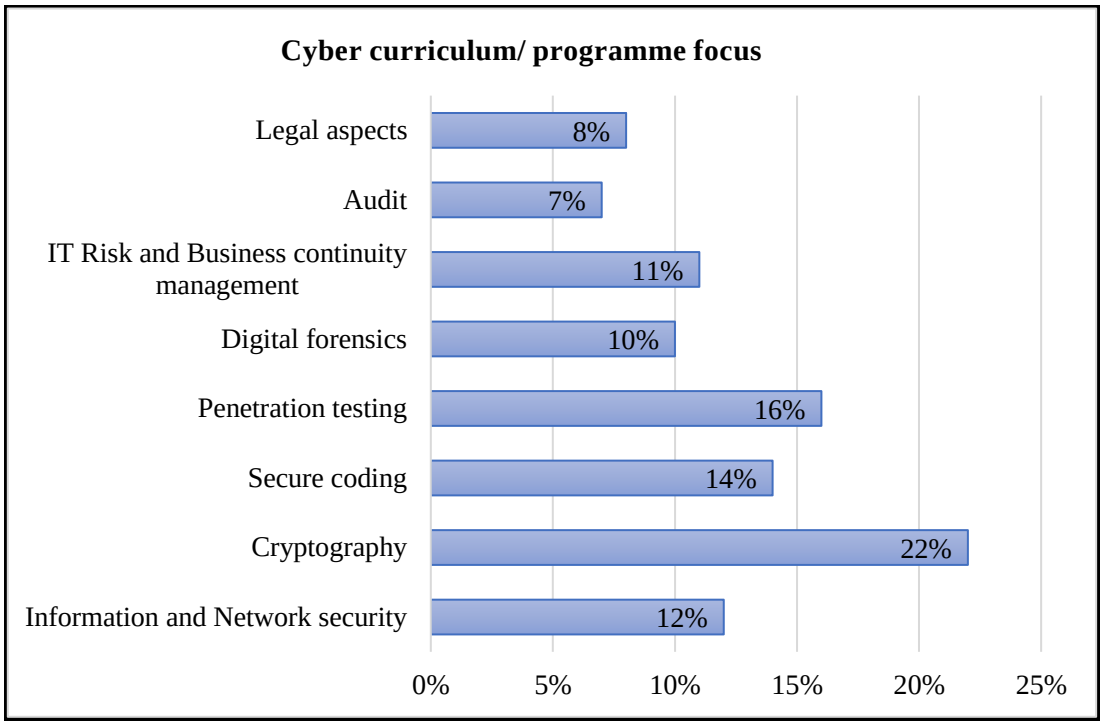

Figure 5.8. The cyber curriculum/ programme focus

To keep up with the latest developments in the field and market demands, master's degree programmes in cyber security are constantly adapting, both in terms of the content of their courses and the structure of their programmes, so that more specialised security courses are incorporated into the set of core courses and that more elective courses are offered.

5.2.9. The select criteria for the CS academic staff

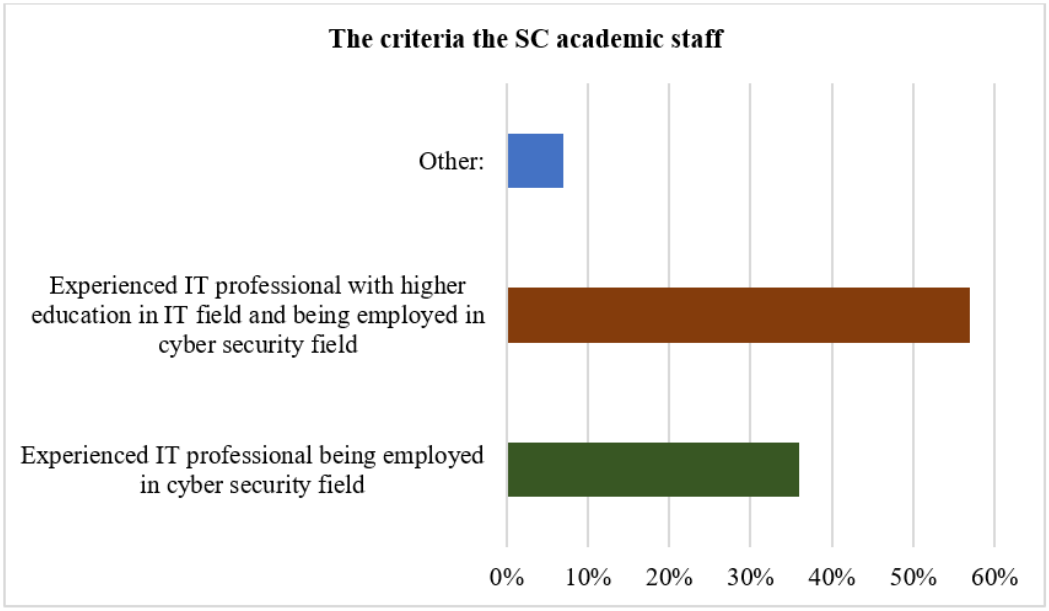

Figure 5.9. The criteria the CS academic staff

5.2.11. The criteria for accepting a student at the CS programme

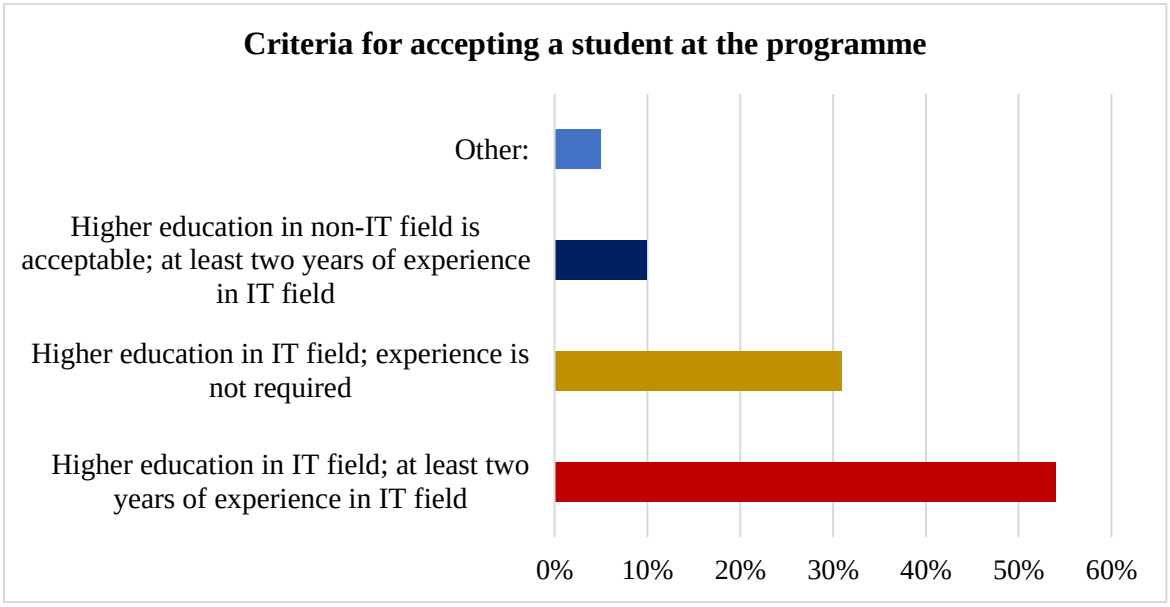

Figure 5.10. The requirements for enrolling a student in a program

According to responses, at least 55% of respondents believed that eligibility for any programs required at least some IT proficiency and some prior experience. Furthermore, 32% indicated that at least students should have some form of higher education but not experience. Overall, at 87% of responds point to some kind IT skill or qualification before enrolling on nay cyber security programme.

5.2.12. Support for the development of the CS courses or programmes

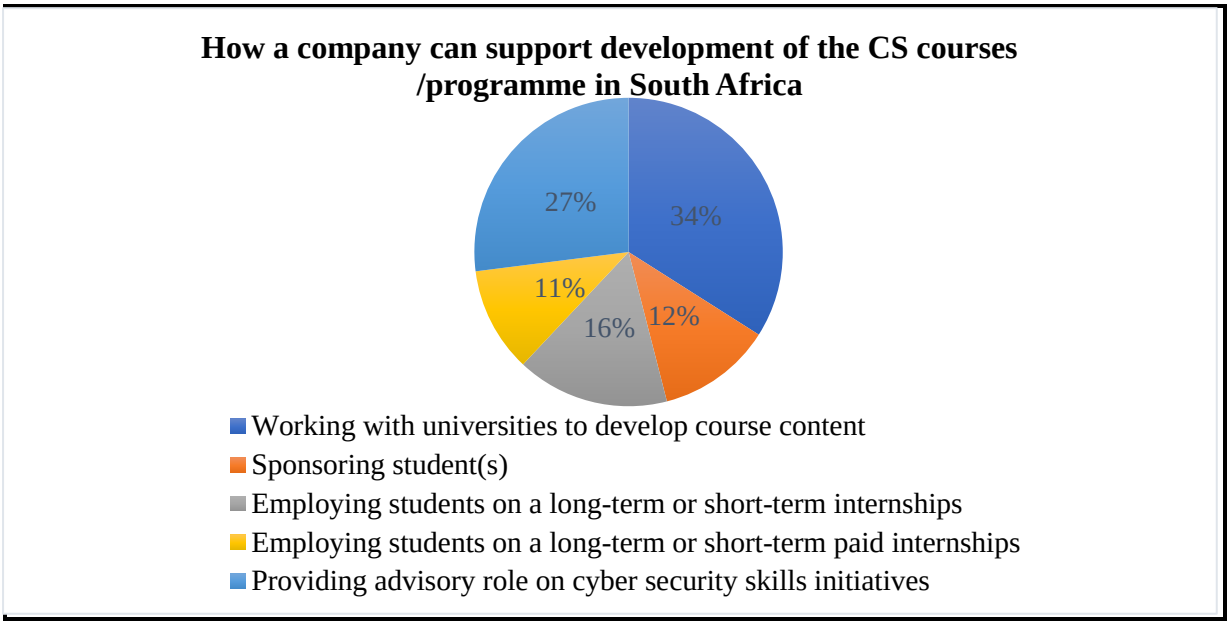

Figure 5.11 CS courses/programme support in South Africa

The findings indicate that cyber security education in South Africa is inadequate at best. As South Africa embarks on several initiatives that will increase reliance on information technologies, demand is expected to rise. It is critical to take steps to develop cyber security capabilities to guarantee the projects will be completed successfully over the long term. The results demonstrate that there is not adequate or any education base for any of the directions of cyber security in South Africa. The need promises to expand as South Africa has been launching various initiatives that will increase rely on information technologies. To ensure long-term effective execution of the projects it is of essential necessity to take measures to enhance cyber security skills.

Furthermore, to promote growth of the CS programme responders are evaluating the following alternatives of combined efforts:

i) Working with universities to produce course content
ii) Sponsoring master student(s) (s)
iii) Employing students on a long-term or short-term internships
iv) Employing students on a long-term or short-term paid internships
v) Providing consultative role on cyber security skills projects.

5.3. Thematic analysis of responses

Saldanha (2013:14) asserts that most of the information gleaned from open-ended responses is qualitative, or nonnumeric. Thus, qualitative data analysis (QDA is required to look over and interpret this data. The term "QDA" refers to a variety of procedures and techniques that aim to provide an explanation, comprehension, and interpretation of the data that has been gathered, in this case, CAQDAS-Nvivo adaption 11, as previously explained.

The content analysis and topic analysis are two of the most popular methods for evaluating responses to open-ended inquiries, as supported by Wiedemann (2013:5). According to the authors, the first method is often used to categorize and measure data and follows a more systematic and mechanical process. The second method, which is widely used to capture the depth and richness of qualitative data, comprises a more flexible and introspective strategy.

As recommended by Sinkovics and Alfoldi (2012:8), the researcher used a rigorous and systematic classification process of coding and theme or pattern identification to produce a more realistic and valid content analysis. These themes or patterns emphasize the reliability and repeatability of observations and subsequent interpretations. According to the authors, categorizing, summarizing, quantifying, and tabulating qualitative data are among purposes for which such content analysis is a particularly useful technique.

Choosing a theme

i) South Africa's CS educational guidelines

ii) The contribution of CS education to the battle against cybercrime

iii) The role of institutions in the development of CS capabilities

iv) Creating a CS curriculum

v) Aligning the academic CS program with industrial demands

5.3.1. CS guidelines for education in South Africa

The data in this aspect was related to whether there are any existing guidelines for cyber security education in South Africa that respondents are aware of.

> All of the respondents—1, 3, 4, 6, 7 and 8—agree that South Africa has embraced cyber security laws and regulations. that the following (draft) laws and rules have been prepared by the Cybersecurity Response Committee (CRC), a strategic organization

chaired by the State Security Agency and tasked with overseeing the implementation of the NCPF:

• The State Security Agency-led National Policy on Critical Information Infrastructure

• The South African Police Service-led National Policy Against Cybercrime

• The Cybercrime Prevention Act, which is being spearheaded by the Department of Justice and the Constitutional Development.

The original draft of the Bill was published in 2015; it was revised in 2017 and sent to parliament one month later.

Since the Bill addressed both crimes and cyber security, it was initially considered to be nonpartisan. However, during the phase of public engagement, worries about people's privacy and freedom of speech developed, causing the Portfolio Committee on Justice and Correctional Services to remove all cyber security-related clauses from the Bill.

The Cybercrime Bill, which addresses only offenses relating to cybercrime, including evidence gathering, punishments, and court jurisdiction, was adopted by the National Assembly in November 2018.

Members 1, 2, 4, 6, and 7

The Cybercrime Bill is now awaiting enactment.

Hacking, ransomware, cyber-extortion, and unauthorized data interception are just a few of the many new crimes that the Cybercrime Bill introduced. In the event that crimes are committed outside of the Republic, the Bill grants South African courts additional authority. The Bill also mandates that service providers and financial institutions maintain any evidence connected to crimes and report offenses to police within 72 hours.

Respondent 1 notes that:

If the Bill is passed, it will repeal the cybercrime-related sections 85, 86, 87, 88, and 90 of the Electronic Communications and Transactions Act, No. 25 of 2002.

Participant 3 notes that;

The Protection of Personal Information (POPIA) Act of 2013 guarantees data privacy, however according to Ewan Sutherland in Governance of Cybersecurity - The Case of South Africa, the act permits "overly extensive exemptions for national security," which includes

cyber security. Sutherland continues by arguing that there is a lack of coordination in South Africa's government regarding cyber security (both at the national and municipal levels as well as with external vendors).

Participants 7 and 8 had similarly sentiments that;

> *Inadequacies in cyber security risk assessments and a lack of transparency are also apparent. Due to its technological complexity, the NCPF also has low legislative control and is being implemented at a gradual rate.* Teaching South Africans about the importance of cyber security and getting people to follow best practices is a significant issue.
>
> *Only 28 governments in the world have a cyber security policy, and South Africa is one of them. Despite the country's flaws, the government's attempts to address these problems should not be underestimated. Shortly, both the NCPF and the Cybercrimes Bill will be enacted.*

There is a general perception that South Africa and Africa as a whole lag behind in cyber security, and the country's government is faced with a number of issues related to cyber security (Participants 1, 3,4,6,7, and 8), including a lack of ICT expertise in some areas (Participants 1, 3), and coordination issues between intergovernmental departments (Participants 4,6,7, and 8). Although the nation has made an effort to tighten and improve its cyber security laws and regulations, there are still many gaps. The ultimate victims of this vulnerability are the citizens.

5.3.2. The role of CS education in fighting Cybercrime

Does cyber security education empower graduates to fight the cybercrime?

Respondent 3 also notes that:

> *Yes, it starts with having a good understanding of what cyber security is about.*

Respondent 1 notes that:

> *Most definitely. It empowers them to know which suitable measures to use for their environment and have a systematic way of implementation.*

Respondent 5 also notes that:

> *Adults are less likely to spend money or time on seminars or programs regarding cyber security, according to a survey on adults and cyber security.*

Respondent 6 also notes that:

> *Cybersecurity education can help to prevent computer game addiction. It's a given that this behavior is bad. Teenagers engage with one another by spending a lot of time on their laptops and other electronic gadgets. Young people today frequently develop addictions to electronic devices and online gaming.*

There are various benefits to completely adopting cyber security instruction in a school, according to the research review. According to a survey, adults are less likely to invest money or time on cyber security lectures or activities. Schools must therefore develop into information hubs for educating the general public about cyber security. Administrators and teachers may create a conversation subject or even an activity around cyber security for their schools. Additionally, schools in Malaysia get government support, allowing them to afford to host such events for the good of the neighborhood. Additionally, enlightening people about cyber security might influence a change in attitude. Everyone who is ignorant of cyber security's importance is a victim of their own stupidity.

5.3.3. Development of CS skills in institutions

1. **How does your institution contribute to building a capable cyber workforce that can reduce the widening skills gap in the cyber security industry?**

Respondent 4 also notes that:

> *Through partnerships with other institutions to provide funding to close skills gap*

Respondent 6 also notes that:

> *By providing grants to institutions to conduct training on Cybersecurity courses. By development of 4IR qualifications which include Cybersecurity.*

Employers at all levels should promote the importance of a cyber security career at their firm, not only in terms of income and perks. One approach is to emphasize the possibilities for further study and growth in one's work. Another approach is to emphasize the purpose of the institution, especially if it is distinctive, as in the case of government CS. There is a rising interest in cyber security jobs among young folks, for example.

> *However, 96% of those polled claimed that feeling personally linked to their employer's aims was as important to them as high pay (90 percent of those polled said this).*

Because of this feeling of purpose, students who have previously shown an interest in STEM fields may find themselves drawn to a career in cyber security. Students who are interested in pursuing a career in cyber security might get an edge by concentrating on the purpose that cyber security professionals serve.

5.3.4. Developing CS curriculum

2. How do you think a cyber curriculum be developed to support a wide- range of security programmes /types within the ODL teacher training curriculum?

Respondent 1, 2 note that:

> *The programs should be developed with industry experts in that field of cyber security*

Respondent 1 note that:

> *Training on Cybersecurity should be embedded in the curricula of most courses of different disciplines. It should only focus on ICT professionals. CIOs, CFOs, CEOs, CROs, CAEs, etc. should be equipped with Cybersecurity skills for maximum important in their CS.*

Respondent 1,5,8 notes that:

> *They will then start enforcing this on their teams so that it is not only an ICT skill. That way we should achieve maximum impact. This should be treated the same way computer training was introduced as compulsory for all courses in universities of technologies.*
>
> *There are a few things you should keep in mind when it comes to appealing to cyber security specialists (i.e., training, professional development, and on-the-job training). To avoid overlooking potential employees, it's critical to set job posting specifications that are specific enough to avoid leaving openings unfilled.*
>
> *To attract the best and brightest in the field of cyber security, companies should look to hire people with appropriate degrees and then train them on-the-the-job.*
> *Finally, firms should turn to their own IT professionals for cyber security employment.*

In many cases, your own workers may already have the appropriate cross-functional expertise you need to fill the gaps in your cyber team with some additional training. To construct a

competent cyber security team, you need take some action and even attempt to develop a basic strategy. Inaction is obviously preferable to this. Hackers will be around for a while to come**.**

5.3.5. Alignment of CS academic programme to industry needs

3. **How can the institution support the alignment of academic programmes and industry needs in cyber security?**

Respondent 7 notes that:

By offering affordable courses and/or training

Respondent 5 notes that:

Through the Research Chairs, e.g., the Chair of 4IR, commence with the development of proposed Cybersecurity strategies and programmes for the country. 2. Using their connections to influence a coordinated drive of the program to influence adoption by many and ensuring implementation is maximised.

Respondent 7 notes that:

Needs to investigate the trends that are currently implemented and go beyond that, they need to set a foundation as in the fundamentals of cyber security, then can go deeper in a particular area of cyber security.

Respondent 8 further notes that:

Through research and identification of the skills in high demand and partnering with business to fund some of the programmes. It is also important that we develop skills in the ETD sector to build capacity to support the evolving curriculum.

Respondent 9 also notes that:

There should be a start on developing a national Cybersecurity strategy and program via research chairs, such as 4IR.

Respondent 3 observation that:

Using their relationships to create a coordinated program effort to inspire widespread acceptance and ensure maximum implementation.

New talent development strategies will also help academic institutions. Companies now utilize different methods to establish their talent pipelines and do not employ many cyber security specialists straight from universities. For higher education institutions to cooperate with companies to establish cyber security routes that better fit industry demands, this circumstance

provides an opportunity. It is possible for higher education institutions to benefit from companies' investment in training the present cyber workforce. A growing number of firms want to train their workers while they are still employed, therefore programs for non-traditional students may need to be extended.

Higher education institutions should also explore creating and implementing new routes for non-technical students. Learning about cyber security dangers from other firms is an excellent method to establish a talent pipeline, according to corporate executives and higher education officials.

Professional societies, associations, and non-profits have a role to play in coordinating information exchanges at the national level. By explicitly incorporating this sharing into the classroom, regional higher education institutions may forge strong bonds with local industries.

5.4. Discussion of findings

In contrast to more wealthy nations with superior national cyber security performance, who have already initiated stronger workforce and educational programs to promote such readiness, research suggests that many less developed countries are progressing slowly toward acquiring cyber competence.

South Africa's cyber security educational status has been examined in this research, and the specific factors that have led to these present situations are discussed. This is a pre-selected group of people who have first-hand knowledge of the problem. Using this data, the study identifies common threads that helped to better answer the research objectives, and then connected these threads to form new categories. During the interviews, these topics came up often among the respondents.

Depending on the source and the complete qualitative analysis that was done (e.g., sample, included site, interview role, institution triangulation through desktop review, and coding), these themes may or may not be significant for the study. To support the conclusions of the literature, the study frequently included citations to the respondents' assertions in the text. The respondents' research is the basis for all conclusions, which inevitably represent their viewpoints and beliefs.

The majority of cyber security courses in South Africa are taught at a fundamental level. There are no undergraduate cyber security programs, and only a few graduate-level initiatives are being tested in a few schools where it could be necessary to assess institutions' readiness.

Bearing in mind that education is now dealing with a number of challenges, including a lack of expertise, a lack of resources, and a lack of governance.

Because the knowledge, experience, and abilities of instructors in the area of information and network security are strongly reliant on academic preparation, most undergraduate programs include security topics into CS and CN courses in an informal manner. A lack of cooperation among academics might lead to security holes and redundant data. Though certain security courses are available, it has been found that many lack depth or breadth owing to a lack of resources, such as laboratories. The safety of critical infrastructure is not taken into consideration.

The results of the data from respondents reveal that academics' efforts to promote cyber security education are being hampered by institutional rigidity and a lack of understanding of need. One must be able to both do and make the decision to prioritize cyber security in order to teach it. The dissemination of cyber security expertise is hampered by the competition with other academic areas because security information is included into CS or CN programs. Recently, a few graduate and undergraduate projects and theses have appeared to support cyber security efforts, and information security is now one of the research areas of a new PhD program in computer science.

Lack of cyber security professionals hinders colleges' ability to educate cyber security in big proportion. It is challenging to overcome this obstacle because of stringent regulations forbidding institutions from integrating industry employees without graduate degrees, high security professional fees, and a severe shortage of capable cyber security specialists across the country.

It appears that academic programs cannot be enhanced or modified to meet the demands of local businesses unless they are intimately related to those needs. Despite government attempts, there is a wall separating the business world from academia that prevents them from working together. Greater cities are more concerned about this than smaller ones are.

Several presumptions about what was expected to be discovered were employed as the foundation for the research approach used for this work. Although a dearth of cyber security staff in educational institutions was anticipated, the lack of interaction between local businesses and institutions was a surprising finding. Although they are essential to the development and success of a cyber security workforce, financial and human resources do not ensure it. Inadequate university policies (such as the difficulties for institutions to assign suitable

professors to teach cyber security courses even when they have them) and people's particular interests may make resources less accessible.

A scarcity of cyber security-trained academics was expected to be an issue, but it turns out that a few of institutions had programs in place to address this issue. Although there are a few short courses in cyber security offered by different institutions, none seemed to offer courses on cryptography.

The study also reveals that the majority of respondents were ready to identify issues that the scientists had yet to discover. That was a pleasant surprise. Academics with subject-matter expertise have all helped to better understanding the market's need for cyber security services. These sources include personal experience (such as hacking incidents) and even consulting engagements from the business world (such as security or educational initiatives). Many colleges are turning to outside resources for support because of the industry's need for speedy answers to difficult problems (the financial sector provides proof of this). Another problem is that some companies' security postures appear lax. Recent surveys indicate that there are several unmet cyber security needs in CS and CN. Surveys are better carried out through a network of institutions than by a single one. Among the lesser-known issues include the language barrier, restrictive academic procedures, and logistical issues.

Although there are no globally accepted standards for CS education in South Africa, examples from other industrialized countries may be instructive. By working together with other educational institutions, treating information assurance (IA) as a multidisciplinary science, promoting IA practice, funding IA research and development, implementing an IA curriculum that has an impact outside of the university, and employing faculty members who are actively engaged in IA practice, research, and publication, accreditation in IA can be improved. These aspects allow for the use of Oxford University's Cyber Capability Maturity Model to assess a nation's cyber security capabilities.

One of the five pillars of this approach is cyber security education. The five phases of maturity are start-up, formative, established, strategic, and dynamic. The lack of educational possibilities and technological advances meant that South Africa's cyber security education could only move to the developing stage.

We may include perspectives from universities with lower academic standards in our research (only 7% of category C and 17% of D) thanks to an in-depth interview approach, a wide range of participant roles, and geographic triangulation. There may be additional obstacles to overcome, such as the absence of academic infrastructure and resources, if other comparable

schools (C and D) are added. It is reasonable to suppose that these universities confront comparable issues, such as a lack of competence, cooperation, and a lack of knowledge about demand.

Since the majority of cyber security responsibilities in South African firms are occupied by IT professionals, I primarily focused on CS/CN programs in our study. As we found in our earlier research (Sinkovics & Alfoldi, 2012), around 55% of the cyber security staff employed by financial institutions are graduates of CS/CN institutions. However, the impact of other academic subjects on the labour market is lesser but no less substantial. Those in the business and telecommunications industries, for example, are among those who routinely relocate large distances.

Additionally, it has been noted that cyber security education can occur in a variety of settings. Success in this depends, however, on CS's current cyber capabilities as well as on the incentives they need to grow and their capacity to do so. Since the majority of colleges do not provide specialist cyber security capabilities, financial institutions and large ISPs have been obliged to educate their technical staff in cyber security in recent years. The financial services industry has a significant demand for cyber security due to domestic restrictions and industry self-regulation. At present moment, there are no cyber security legislation in place for the telecommunications business, although several major ISPs are considering entering this sector. National security considerations, internal politics, and geopolitical goals all play a role in the military's decision to invest in cyber capabilities.

The nation as a whole has to make significant efforts to increase cyber security education (e.g. MS programs, research initiatives, and specific security courses), even though the most technologically proficient universities have created unique approaches for handling cyber-security concerns. These initiatives must consider how cyber security education is developing.

5.5. Implications of the findings

Industry has been finding it difficult to produce capable cyber security personnel partly because of the short supply or inadequate preparedness towards cyber attack pandemic. One could also view this shortage as a management decision not to prioritize cyber security personnel. World Economic Forum (2023) highlight encryption and cybersecurity as 6th critical skill that will be adopted globally between 2023 -2027 as many organisations adopt technologies like internet of of things, cloud computing on e-commerce platforms that are prone to cyber attacks.

The industry has come to grasp with the viciousness of cyber attacks and are strongly suggesting that there are certain skills that must be top priority in order for industry to deal with cyber attacks. Even though their prioritization is re-active rather than preventative it is worth noting that the skills agenda has become important. Highlighting cryptography, penetration testing and secure coding is a good example of preventative thinking meaning that these entities will be putting measures in place to prevent cyber attacks from happening by employing more complex cryptos, writing software with robust and tested security parameters ad continuously testing oneself to identify vulnerabilities. Reactionary thinking like digital forensics and business continuity management is also vital from a learning curve perspective and organisation maturity. All these areas are a clear indication of skills demanded by the industry.

Interesting though that the very same skills forecasted as in high demand in the future are the verry same skills that are scarce. This thesis therefore has a great opportunity to make an impact in assisting with a framework of producing these scarce skills to meet the market demand.

One is not surprised on why the above skills are scarce because this figure 5.5 highlight clearly what is being taught at our educational institutions varies with what the future skills demand looks like. This then answers the philosophical question of "Why" our CS offering is falling of market expectations. There is a vast difference around technical skills needed by the industry forecasts against what our academic institutions are offering.

In addressing these skills shortages there is an interesting contrast of current vs future strategies. There is general acceptance for external training particularly abroad. This implies a need to align ourselves with international standards.

This alignment is largely along the skills in short supply i.e. secure coding, penetration testing, cryptography ad digital forensics. This implies therefore that our local educators must align the CS offering and match industry expectations. The focus area for cybersecurity offering or program has penetration testing as one of the focus area. Within our current CS offering in our colleges, Technikons, universities, this focus area is non-existent along with other focus areas of secure coding, digital forensics. These types of focus areas are, however, available as industry qualifications on imported curriculum.

It is also interesting to note that the select criteria for academic staff is heavily reliant on IT experienced instead of cyber security experience. These skewed criteria will undoubtedly produce workforce not well educated or equipped in the field of cybersecurity

With some respondents highlighting that only 33% of companies work with universities on curriculum development is also problematic. KPMG Global Cybersecurity Task Team (2022)

notes that organisations need to work towards cultivating talent pipelines by partnering with universities, developing in-house talent and offering attractive remuneration. In other countries like China, Japan; there are academic boards that are occupied largely by companies solely because they source heir graduates from such an institution, and they get involved in approving any academic offering. This is the reason why the demand is ahead of the supply.

5.6. Chapter conclusion

Technical factors are given a lot of attention in the scientific field in the United Kingdom, where research has achieved a high level in the numerous research facilities located in the country's borders. Many courses offered by the computer schools include legal and management components, helping students to get a more comprehensive grasp of the field, and some of these courses are available to students with an undergraduate degree in economics and management, as well.

The legal industry has a strong understanding of IT security, and research has shown an interest in the new dangers and implications that arise from the usage of new technology. The management sector of IT education should be upgraded to produce more skilled students who can meet the demands of businesses for IT managers. The courses run in conjunction with the schools of computers are not adequate to generate a new generation of managers capable of dealing with all of the management issues created by the new technology. This necessitates the opening of new courses devoted only to the management of information and sensitive data, as well as the estimation of the appropriate level of investment in IT security and information flow monitoring and analysis. One way or another, law students should be given greater technological expertise, and computer schools should teach more about legal challenges.

CHAPTER 6

PROPOSED MODEL OF CYBER SECURITY EDUCATION

6.1. Introduction

This chapter presents the proposed model of cyber security education that can be looked at from policy and later academic points of view. The construction of the suggested model is the result of a thorough literature analysis, the study's theoretical framework, and field data. The model is summarised diagrammatically, and each element discussed.

6.2. Proposed cyber security education paradigm

The diagram below is an illustration of the proposed model for cyber security education.

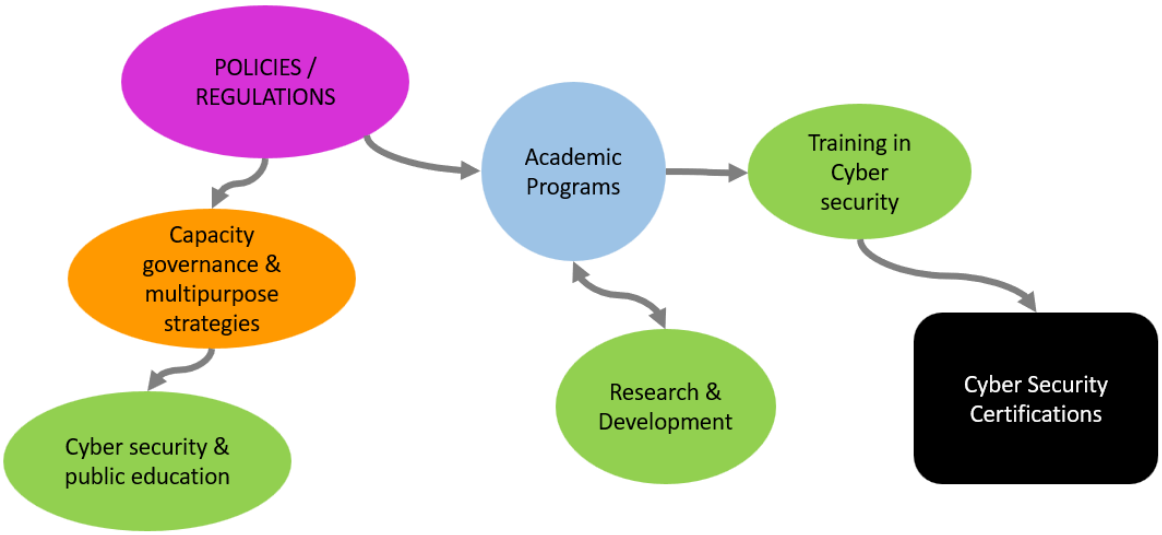

Figure 6.1. A model of for advancing cyber security education

Source: (Own design)

The model is product of the views that the universities alone will not be able to deliver the successful enhancement of cyber security education that will be required to be achieved in the future (Calandro, Manyame & Gillwald, 2019). It might be necessary to involve a variety of

stakeholders in this. The six dimensions of capacity governance, academic programs, training, certification, research, and development (R&D), cyber security awareness, and cyber security awareness training make up national initiatives to advance cyber security education (and workforce capabilities), according to Calandro et al. (2019). The possibilities that are then presented in terms of these characteristics are captured by this model.

6.2.1. Administrative rules and policies.

Universities should review and possibly relax policy restrictions (stringent copyright laws, caps on the number of specialized professors that can be hired, and restrictions on the distribution of university funds) that limit innovation and collaboration with outside organizations, deter students from enrolling in security courses, and prevent investment in cyber security research. In addition, initiatives to promote inter-university collaboration are required. Distributing knowledge across university departments could help to integrate efforts to improve the institution's grasp of cyber security. At least one university presently employs this method, which enables students with different degrees to take integrated cyber security courses that cover the same material.

Networks could encourage national and international collaboration beyond university-level efforts. Academic networks in South Africa could be expanded to actively address cyber security initiatives across the country. To assist South Africa in building its capacity in a number of areas, such as science and technology policies and research institutes, scientists and academics from South Africa and elsewhere should collaborate and establish a network.

Wright (2015) claims that the Computer Emergency Response Team (CERT) at Carnegie Mellon University was established in 1988 with the express purpose of addressing cyber-security issues. The teams that respond to these incidents are now referred to as CERT, a term approved by Carnegie Mellon University, or Computer Security Incident Response Team (CSIRT). CERTs have proven to be effective tools for promoting national cyber security in a variety of economic contexts and dimensions (Parekh, Pawar, & Munot, 2016).

The CERT programs have provided support for a wide range of educational initiatives in many different nations, such as educating university faculty about information assurance, creating survivability and IA curricula as well as educational materials, establishing regional academic clusters, and promoting initiatives that help colleges and universities (Parekh et al., 2016). Since many nations now use CERTs, they are no longer just a resource for wealthier nations

when it comes to cyber security. CERTs today serve a significant role in promoting cyber security knowledge and awareness in developing countries like Oman, Cameroon, Rwanda, India, and others. In fact, the Oman national CERT provides cyber security training in a variety of areas, including awareness and credentials, despite having a GDP that is nearly five times lower than South Africa's (World Bank, 2021).

Benchmarking to cyber security readiness, Oman's national CERT has helped the country rise to third place globally and to the top of the Arab region according to the ITU's global cyber security index (World Bank, 2021). Strengthening countries to perform at a high level when it comes to identifying and developing their cyber capabilities can be accomplished with the help of an effective and well-managed CERT.

Therefore, stronger capabilities are required in South Africa for prospective CERT assistance of cyber education. The CERT with regulatory jurisdiction, established in the country in 2015, but its scope is confined to only the telecommunications sector and a few public sector areas. However, it fulfills its goal by collaborating with key players in the public, private, and nonprofit sectors to identify and mitigate cyber security threats. However, this CERT might be improved academically to solve the issue of a shortage of specialists at universities

6.2.2. Capacity governance and multipurpose strategies

The NICE framework, developed by Sinkovics and Alfoldi in 2012, divides cyber security workforce functions into seven categories: securely provisioning, operating, and maintaining, protecting, and defending, investigating and gathering data, gathering and operating data, analyzing and overseeing. However, monitoring and development skills are especially important in underdeveloped nations when there are gaps in legislation and legal frameworks addressing cyber security challenges or flaws in such governance tools. It is common knowledge that certain categories of labor responsibilities cannot be supported by the current pool of trained experts. It is crucial that South Africa carefully evaluates the needs of such highly qualified individuals to assist in the creation and implementation of national cyber security policies and standards in the medium and long term.

First, despite having a national cyber security policy framework to outline a focused and consistent approach to guaranteeing the security of the nation's cyberspace, South Africa needs to develop a national cyber security policy that lays out governance principles and encourages tools that can develop cyber capabilities in academia. This plan should list the critical

infrastructure areas that require immediate attention in priority order, followed by a list of the cyber security knowledge and skills that should be developed in schools, colleges, and other CS for use by students, professionals, and the public.

To address the most urgent needs of the nation, South Africa must invest resources in educating teachers about computer systems and network security, setting up cyber labs, and launching cyber research and development initiatives. This can be accomplished with the help of private funding, educational R&D grants, and scholarships. The South African government already supports study abroad in the field of applied information security to encourage students to pursue degrees in it. Equipment donations from the public and private sectors should also be promoted. After removing the obstacle to industry-academia collaboration, self-funding research collaborations should be investigated. Early instruction in computer science and cyber security should be a part of all school curricula.

So that they are more likely to pursue it, students in school should be made aware of the opportunities for a career in computer science and cyber security. Professionals in computer science and cyber security should be encouraged to take part in public awareness initiatives and conversations. Or, to put it another way, because the majority of high school students didn't take computer science classes in their early years, they have the wrong impressions about CS programs. The notion that computer science is solely about studying software programs turns off some pupils.

University campuses in big cities need to create incentives that encourage the establishment of mutually beneficial business-university connections. One strategy the institutions can use is to connect with the industry through alumni; another is to identify real-world issues in the sector and propose initiatives that will benefit both parties (consulting services). Additionally, the actions listed below can be used to strengthen ties with the sector:

- Participating actively with university contractors who have the potential to forge technology links. Universities, for instance, are clients of Internet service providers that can perhaps offer technical advice on cyber security issues in the telecommunications industry.
- bringing in cyber security experts from established academic institutions.
- planning conferences; and
- requesting contacts from the industry.

• promoting courses that the market demands, forging connections, and maintaining those connections.

• Forming university coalitions to take on commercial actors in concert.

Once such initiatives are in place colleges should pursue industry commitment for:

• Providing insightful information on the most important industrial cyber security demands and issues, as well as providing accurate survey responses. The gathering of this important data using both approaches would significantly improve understanding of the need for cyber security.

• By doing this, colleges might better match their curricula to market demands.

• Supporting research projects in cyber security and other educational programs, like cyber security labs.

• Fostering student training through apprenticeships and internships (see subsection "Cybersecurity training").

Educators might take action to prioritize cooperating with prospective employers (commercial and public) more highly among activities to advance cyber security education. As previously said, there are a number of possible advantages, including a better understanding of staff needs and financial support, a type of resource that is required by a significant share of colleges taking part in our study.

Establishing linkages between academia and industry is a process in which the government plays a significant role. To address national cyber security educational needs and objectives, government, business, and academia must collaborate in a multi-stakeholder environment. There are many methods to show private and public support for improving cyber-security education, thus this thesis will focus on a number of different aspects of its growth.

6.2.3. Cybersecurity awareness and public education

A common theme across is the urgent need for more national attention to CS awareness. At least some higher education institutions are already educating its own audience (through online education) in academic settings (Universities of Pretoria, Johannesburg, Witwatersrand, and Cape town) and this is a model that other institutions can follow.

The National awareness programmes (Rwanda), cyber hygiene campaigns, and national cyber security awareness week are some of the global strategic initiatives that have been effective in Africa, and South African academia and policy can learn from them. Such campaigns must choose their target demographic, themes, and delivery strategies to be effective. Others contend that in addition to adults, the audience should also include people working in the business, decision-making, and justice sectors of society. Current domestic cyber dangers should be included, but discussions should also consider global developments in this area. Basic details on attack tactics (such as malware infection and social engineering), outcomes (such as fraud and the invasion of privacy), and mitigation techniques (such as patches and password best practices) should be included. In developing nations, education can be delivered through schools, radio (in Cameroon), television, and the internet. Like formal education, the means used to disseminate awareness materials are essential to achieving the goals. Potential teaching aids for cyber security education include videos, cartoons (in Brazil), and analogies based on pre-existing mental models of the physical world (Pruto & Batoli, 2006).

The methodology presented by Kortjan and Von Solms (2014) offers strategic insights into addressing South Africa's cyber security awareness and education needs. As essential as this information is, using it in a developing country must consider the national skills that are already in place. If you are a victim, you're going to be targeted by a sophisticated opponent, and you're going to be able to adjust your defenses, so you're not going to be able to get rid of the problem with awareness alone (Sheinov, 2019). Despite this, appropriate understanding and education can help to better fight against some types of attacks (such as malware infection and social engineering).

6.2.4. Academic programmes

It is important to strengthen the following relevant content in undergraduate programs: (i) cyber security content included into introductory CS and CN courses; and (ii) security concerns covered in cyber security courses. Both strategies need to be improved. In this instance, as suggested by interviewees, incorporating security information into itineraries would be a suitable substitute for creating security expertise. This initiative will probably be very beneficial to experts in the local industry, which frequently hires specialists for multi-functional tasks, since it might give them solid CS or CN expertise as well as security skills (Bajaj, 2010). At a university with a proven track record of success in the field, an undergraduate cyber security program may be feasible, especially if it draws on the knowledge of many departments.

Before proceeding, nevertheless, careful investigation of the South African labor market situation is necessary.

MS programmes should be bolstered, and new ones should be launched in cities where they aren't currently offered. Of those surveyed, 42 percent said that creating MS programmes in cyber security would be a good first step toward improving general security education. Universities have more discretion when making decisions at the graduate level than they do at the undergraduate level since graduate programs are typically self-funded. A university is an exception if its classification prevents it from providing graduate programs.

It is easier and more dynamic to it adjust masters' programmes than is in undergraduate programmes as more master's degree programmes in information security are needed (Michael et al. 2017). The educational system needs to contain a wide range of academic security content, including those related to industrial systems, electronics, tele-communications, and criminal justice. There are worries regarding the lack of training for law enforcement officers as well as the lack of cyber risk education in the workplace.

Even while it is evident that the current shortage of specialists hinders such projects, it should eventually be possible to demonstrate the situation. Faculty members instructing security-related courses at institutions might benefit from current master's programs with improved capacities for explicitly training educators (Michael et al. 2017). To carry out this initiative, trainers with knowledge in cyber security may be found both inside and outside of South Africa. Two potential sources of experts are foreign-trained security professionals who are already employed in the nation or who are returning as part of government scholarship programs. The other is the temporary importation of foreign subject-matter experts, a strategy the government is now employing when promoting research in other fields of science as well.

Long-term imports may be difficult due to the existing global lack of cyber security expertise (Wright, 2015). Internationally qualified security personnel. These initiatives may enable national master's degree programs to be better adapted to the needs of South African society today. A cyber security master's online from a foreign university is an additional choice.

International education has been seen as a useful tool to assist students in tertiary domestic education to help them reach higher levels of maturity. When importing academic curricula, care should be taken to adjust designs to the domestic situation. Some interviewees highlighted The Joint Task Force on Cybersecurity Education and The Association for Computing Machinery (ACM) as resources for cyber security subjects in computer science curricula. A holistic approach must incorporate the expertise of all society segments (Parekh et al., 2016).

South Africa needs to identify the knowledge and skills that could support adequate curricula; therefore this endeavor must be started because current local approaches lack this information.

To deploy cyber security curriculum, it is necessary to identify and incorporate effective learning methods. For example, case studies from the actual world and practical simulations should be considered in academic instruction (Wright, 2015). It is also possible to use adversarial thinking to enhance the key ideas that allow us to understand system vulnerabilities so that we can better prepare to deal with emergent threats, rather than just known ones. While acquiring new skills may take some time, it is critical to begin taking practical measures today and to begin or at the very least examine more difficult efforts.

6.2.5. Training in cyber security

Faculty members who lack prior experience in cyber security will benefit from specialized training, which will help academic departments create more comprehensive courses. In this case, a CERT's support in educating educators can be quite helpful. Like this, the establishment of labs and real-world experiences earned outside of the school must support students' practical cyber security training. It should also be taken into consideration to offer incentives to local businesses, such as paid internships and trainers, to support educational programs like this one:

- Encouraging academics to impart their know-how through time, as well as government agencies that support growth.
- Involving international partners in the initiatives, such as IBM and Microsoft
- Sharing the training, which at least one other organization has already adapted.
- Infrastructure like forensic centers and training programs should be built.

Virtual training environments can be implemented through:

- Increasing the number of security workshops
- Increasing rivalry in the security industry
- Creating and promoting apprenticeship programmes to give students practical experience in the field of cyber security.
- Focusing on hands-on, practical, and intense security education (Parekh, et al., 2016).

Several governments have recognized the advantages of apprenticeship programs to enhance the practical-technical training of cyber security experts. The British government supports cyber security apprenticeships, making them publicly sponsored in the country. As an

illustration, community organizations in the United States have started to provide cyber apprenticeship programs, funded by business alliances.

Finally, training is necessary to increase the standard of practice in business and law enforcement. Controls that ensure adequate levels of excellence should be examined considering concerns regarding the quality of commercial training.

6.2.6. Research and development

The growth of cyber security research in South African institutions is a significant issue since high-quality research must rely on existing resources and infrastructure, such as skilled researchers, funding, research centers, and real-world projects. A national program for cyber security research and development must be established. However, universities' current initiatives to conduct information security research might be strengthened and expanded, which might pique the interest of more faculty members in the creation of instructional programs. For the protection of infrastructure, it is imperative to do research in both the public and commercial sectors.

6.2.7. Cybersecurity certifications

Others think students should be encouraged to pursue security certifications as a means of enhancing understanding, even though marketing professional certificates may not be institutions' primary responsibility. Some developing countries looking to improve their cyber security performance are considering government and CERT support for international accreditation programs (like Oman) and certification programs (like Rwanda). Following professional security associations with affiliation for students at a low fee should be encouraged to increase accessibility (Kortjan and Von Solms 2013).

6.2.8. Conclusions

The inadequacy with which South Africa's educational system has failed to appropriately prepare students for the threat that cyber security poses underscores the necessity of a deliberate approach to the enhancement of cyber security education in both formal and informal contexts. Only a small number of universities (such as those in the financial sector) have embraced a comprehensive national academic approach to cyber security education as a result of heightened public awareness of the threat that cyberattacks represent to the nation's key infrastructure.

In order to meet the needs of both groups simultaneously, educators and society as a whole must address the growing problem of cyber security. Cybersecurity education can be advanced by utilizing institutional resources including academic programs with strong ties to societal demands, academic infrastructure, and a robust research foundation.

Because South Africa is still in the early phases of creating cybersecurity infrastructure, deali ng with the issue of cybersecurity is particularly tough in the country. A scarcity of Cybersecurity trained faculty and technical resources has resulted in colleges and universities being unable to conduct academic education (courses and training).

Lack of collaboration between universities and businesses, especially in large urban areas, makes it hard to take actions that promote growth (such as better understanding demand). When comparing South Africa to industrialised nations with established, top-tier educational systems, the differences are striking when it comes to the cultivation of a cyber-savvy workforce.

Several organizations, including private security companies, tech companies, and military organizations—all of which are actively engaged in cyber operations—conduct cyber operations in those nations. Several nations can nevertheless excel in the realm of cyber security despite their constrained personnel and financial resources. For instance, emerging nations can learn a lot from Oman and Malaysia about how to improve their economy.

Although there are many tactical recommendations for handling this problem, relatively little study has looked into the factors that make it difficult for cyber security education to take place in a developing country. To close this gap, the authors of this article spoke with educators in South Africa, a developing nation, to get their viewpoints on the issue.

Financial sector stakeholders have reported a lack of qualified cyber security professionals in the local labour market, and this study investigates the causes of this shortage and possible solutions. The findings of this research provide important information for understanding what motivates young people in developing nations to study information and cyber security. All governments have high expectations, but those in developing nations, which have fewer tools at their disposal, must make do with what they have. Cyber threats, both accidental and malicious, are impossible to fully quantify. However, patterns on a global scale show that risks are increasing.

It is important to develop and discuss a national cyber security policy that sets concrete objectives and gives guidance, as well as ways to work closely together between academia and

industry. Additionally, when instructors are receiving training in the area of cyber security, relevant curricula should be developed.

CHAPTER 7

CONCLUSIONS AND RECOMMENDATIONS

7.1. Introduction

This chapter will present the significance of the contribution of this study.

Drawing from literature, the study sought to answer the following questions:

i) **What are the existing guidelines for cyber security education in South Africa? To what extent does the cyber security education empower graduates to fight the scourge of cyber crime?**

It's critical that all South Africans understand how to protect their smart gadgets against cyberattacks. A high level of security awareness and understanding is required to do this task. South African schools do not have a formal cyber security curriculum currently. As it presently stands, colleges and institutions are the only ones that can teach students about cyber security. Since just a minority of South Africans attend university-level computer courses, this strategy has had little impact on raising awareness of cyber security threats and how to prevent them.

ii) **How can South Africa higher education contribute to building a capable cyber-workforce that can reduce the widening skills gap in the cyber security industry**?

In addition to the central research question, three sub-research questions will further guide this study:

i) In which way can cyber curriculum be developed to support a wide- range of security programme /types within the teacher training curriculum?
ii) Why South African computer security offering is falling short in meeting the demand for capable cyber personnel?
iii) What should be the structure for cyber security discipline and a model of curriculum that outlines key dimensions of current industry trends?
iv) How can the institution support the alignment of academic programmes and industry needs in cyber security?

The answers to these questions point to the need for increased training and education opportunities and the promotion of cross-functional expertise on IT and OT security. In its new

strategy, it has made strengthening internal capabilities a top priority, and it has launched numerous campaigns to raise consumer awareness and encourage more responsible Internet use. To address the shortage of cyber security professionals, which threatens both economic development and national security, it is also promoting and evaluating cyber security education. The CS programs need not stay rigid against a changing cyber terrain. IT has to align to international standards and trends to mirror the fluidity of attack surfaces and prepare graduates for complex threat variants. The recommended framework does map feedforward and feedback of research and development into curriculum development and teaching thereof.

Many countries, including the United States and the United Kingdom, are trying to raise public awareness about cyber security careers, but the promotion of these programs is disjointed and there is no international standard.

The government of at least one country has begun investigating the issue. In order to increase the number of students studying cyber security, governments at all levels have launched awareness campaigns. To give just two examples, in Canada and the United Kingdom, cyber education is now being implemented for students as young as eight years old. As encouraging as this is, it does nothing to address the pressing need to train the next generation to handle cyber threats.

In one of the subgroups, work has begun on a technical report about cyber security education and training. Released when complete, it will define the "why," "what," and "how" of cyber education and training to improve the current state of affairs. A well-informed and competent workforce that can defend business and society is essential, and this researcher will explain why cyber security education and training is so important. It also highlights the importance of making cyber security education a strategic priority in workforce development for organizations of all sizes and in all fields of endeavour.

The available options for formal education, professional training, standards, and recommendations will be outlined in the recommendations. It can be used to learn where there is room for growth and development. In addition, it will delve into the more specialized areas of cyber security training that are essential for effective cyber defence.

7.2. Theoretical conclusion

There are two major contributions that Bloom's Taxonomy made to the field of curriculum development. First, it can be used as a rubric by teachers to determine the course's intended

learning outcomes and how to assess the course's instructional strategies. Second, it provided concrete examples of how security-related and emerging cyber security themes can be analysed in an IT curriculum that has been accredited by the Accreditation Board for Engineering and Technology.

If you are a teacher at another institution and would like to include cyber and security-related topics in your lessons, you can do so with the help of the IT Security-related and Cybersecurity Curriculum Taxonomy. It's possible, as seen in this research, that some topics will be emphasized excessively while others are neglected or that some topics will be entirely left out of the curriculum. Schools seeking ABET accreditation must place a premium on ensuring that curricular themes are assessed for effectiveness. In the second step, teachers may apply the themes to the student learning taxonomy to gain insight into their students' learning processes. This finding suggests that more in-depth training could help students get ready for the workforce. Further, it can help educators consider how to incorporate timely topics in cyber security education without increasing course load.

This analysis of the literature shows that using Bloom's taxonomy to structure instruction in cyber security could help bring it in line with the needs of the industry. Academic cyber security and the next generation of cyber workers can be brought together through the application of Bloom's taxonomy. To complete Bloom's taxonomy, "cognitive reasoning" can be added if "technical and human-centric skills" are combined (Whitman & Mattord 2013). In the field of cyber security, there is a lack of a clearly articulated curriculum or systematic approach that covers all the skills required to carry out the various tasks associated with various job profiles.

To help stakeholders enable cyber security professionals to perform at their best, we've incorporated the NICE Framework's KSAs into this framework (Whitman & Mattord 2013) Government and non-profit CS in the field of cyber security can use a mapping of the NIST NICE KSAs to Bloom's taxonomy to identify skill shortages and related capability gaps. Improving students' mental faculties is a key component of creating a robust cyber security workforce, and that's exactly what this curriculum aims to do. This study makes good use of Bloom's taxonomy to assist future cyber security professionals in planning their careers by identifying the various job responsibilities that can be performed by individuals with different skill sets. However, due to the dynamic nature of the cyber security landscape, this approach will fall short of being an ideal means of closing the talent gap.

Numerous reports have highlighted the need to revise existing cyber security curricula to accommodate the dynamic nature of online dangers. There is a growing need for highly trained

cyber security professionals who have the necessary Knowledge, Skills, and Abilities (KSAs) to ensure the safety of all electronic data transmissions. Given the dramatic increase in the number of people learning about cyber security on their own, it is important to evaluate the current state of cyber security education. Since the intended rubric and skills matrix does not mandate an infinite number of KSAs, they can be used to investigate a wide range of occupations and activities in the field of cyber security. Therefore, it may be possible to align industry needs with curriculum goals, thereby meeting the growing demand for cyber security professionals in the future.

7.3. Empirical conclusion

7.3.1. Education, training, and awareness in security

Educating and training employees in a way that is specific to the organization's structure and operations is essential to the success of any security framework. The number of security breaches can be reduced if employees are provided with security education, training, and awareness (Whitman & Mattord 2013).

The goals of security education, training, and awareness are to make people more cognizant of the importance of safeguarding system resources, to equip them with the knowledge and abilities they need to carry out their duties in a more secure manner, and to equip them with the expertise they'll need to design, implement, and manage security programs for computer systems. A study conducted by Michael and co-workers in 2017 (Michael et al.)

7.3.2. Applications to the Practice of Professionalism

There are several IT leaders in the education and training sector who, according to this study, are concerned about the safety of their organization's data because they lack the expertise to implement effective cyber security awareness and training programmes. A lack of thorough cyber security awareness and training programmes to protect information systems and data has been identified as a major problem for many businesses, according to recent studies. The training providers that took part in this study all had solid SETA plans in place to protect their data and systems. Since all four companies operate in highly regulated sectors, the panellists agreed that conforming to federal, state, and industry standards is essential to the success of any SETA strategy.

All study respondents who described their SETA approaches emphasized the urgent need to implement all-encompassing, persistent, and topical cyber security awareness and training programmes. Participants also noted the importance of sharing expectations and results, as well as learning more about potential threats, weaknesses, and hazards. IT managers in both regulated and unregulated industries can use this research to develop and implement a training and awareness program for information security.

Businesses that participated in the SCT study agreed that its guiding principles should be used as the basis for their own cyber security awareness and training initiatives aimed at protecting sensitive company data and systems. Companies in a wide variety of sectors can gain from exploiting SCT's constructs in order to encourage particular kinds of cyber security behaviour. If IT leaders at an organization assume that their staff members are autonomous agents whose actions and knowledge acquisition are guided by a triadic reciprocal determinism model, they will be better equipped to implement SETA methods and design environments that foster desirable behaviour.

In training businesses, self-efficacy, self-regulation, social learning, and expected results have all proven useful in encouraging employee behaviours that protect an organization's information systems and data. This research could lead to improved SETA programs, less careless behaviour in cyberspace, and a greater emphasis on the human element. The user is the organization's weakest link because they lack information about cyber security best practices, threats, and vulnerabilities (de Bruijn & Janssen, 2017). Inappropriate cyber behaviour has resulted in severe damage to national security (Gootman, 2016) and hefty financial penalties (Plachkinova & Maurer, 2018). Reference: (Jeong et al., 2019). The hospitality industry is highly regulated, with rules like PCI DSS and newer ones like GDPR. It is especially important for hotels to be aware of their GDPR responsibilities due to the high penalties and other costs associated with data breaches (Wilson, 2018).

In addition to the fines and reputational and trust losses that may occur because of a data breach, a business may see a drop in revenue. In addition to hurting the company itself, large-scale cyber incidents can have far-reaching effects on local education and training. The local and state economies, as well as the careers of training industry professionals and the safety of their clients, all benefit directly from well-executed SETA programs.

Personnel must receive consistent and relevant training on a regular basis to successfully implement a SETA program. According to the results of this survey, all IT managers consistently apply timely and pertinent education. Participants P1 through P6 demonstrated

that they had received relevant training by making use of training materials in the classroom that included problem-based scenarios that required hands-on application. Test phishing emails can be used as a teaching tool and to raise awareness, as was found in further research. In this analysis, SCT was used to look at the data. One way to promote the desired attitude and actions is to increase an individual's confidence in his or her ability to do well in SCT. Effective cyber security self-efficacy can be fostered through scenario-based training designed to facilitate the transfer of knowledge. If workers are confident in their ability to handle cyber threats, they are more likely to act in a proper manner.

Afterwards, the respondents' CS displayed a tendency toward self-control. The CS used SETA strategies to foster a culture of voluntary self-control among its staff. Organizational training materials, documents, and practices that highlighted threats, vulnerabilities, and risk influenced self-regulation. The purpose of the CS was to educate workers on the potential hazards and risks they faced while performing their jobs. Each participating CS analysed potential risks to their CS and then created training materials that accurately portrayed those risks to their staff and trainees. Staff training in the recognition of potentially hostile activities and the appropriate response led to improved self-regulation. The ability to safeguard valuables was strengthened by training oneself in self-monitoring, self-diagnosis, and personal reactive systems.

Participants' SETA strategies were most affected by the SCT's focus on outcome expectations and social learning from the SCT construct. Participating businesses shed light on how poor conduct affects bottom lines, reputations, and the bottom lines of their employees, customers, and the public. Participating CS imposed penalties on those who engaged in inappropriate behaviour to deter similar incidents in the future. The most crucial part was carrying out the consequences, such as cutting off their internet access, making them take extra classes, or even firing them. The participating CS also shared their motivations for and hopes for implementing social learning to improve citizens' online behaviour. Understanding the harm and consequences caused by one's actions in the workplace is a powerful motivator for employees to engage in social learning.

The results of this study provide an examination of the procedures used by the participating CS to implement the SETA programmes. In addition, this thesis details how SCT can be used to propel SETA safeguards for protecting critical information and assets. The findings of this study may prove useful to IT managers all over the world as they provide them with new tools and methods to improve their operations.

Both the SETA program and the cyber security programs of organizations stand to gain from these newly disclosed strategies. This research has implications beyond just the SETA program, including the education and training industries.

Society can benefit greatly from training companies that employ effective cyber security awareness and training tactics. Better behaviour at home may result from increased cyber security education for workers. Children need to be taught about cyber safety to protect themselves in the online world (Rahim, Hamid, & Kiah, 2019). It's crucial for households to be informed about and prepared for cyber threats (Hermogeno, 2019). Children and their families can gain from the knowledge gained through SETA programmes, which may help lessen the impact of harmful situations on families.

Increases in the cyber security knowledge of staff, customers, and the public can lessen the likelihood of security breaches occurring. Projects funded by the Small and Medium Enterprise Technology Assistance Program (SETA) protect businesses of all sizes from cyberattacks (Bada & Nurse, 2019). SETA initiatives can lessen the frequency with which cyberattacks on healthcare infrastructure damage or destroy vital equipment, thereby reducing the likelihood of patient harm (Schwartz et al., 2018). The successful implementation of cyber security awareness and training initiatives has led to higher stock prices (Berkman et al., 2018). Increasing the efficacy of SETA programs protects users' private data (Hermogeno, 2019). It is possible that improved SETA implementations that protect social programs will be beneficial to customers, employees, and society at large.

This study has the potential to shed light on a particular area of social cybernetics. The logical (information), physical (information), and social (social) layers make up Cyberspace's four distinct layers (Zeleke, 2019). Everything related to human beings—their actions, thoughts, and mental processes—is considered part of the social subdomain (Eggenschwiler, 2018). Cybersecurity's worth is lowered because its social and organizational aspects are ignored (Dawson & Thomson, 2018). Understanding the social subdomain of cyber across businesses, employees, and customers will lead to a deeper comprehension of the entire cyber domain.

For the benefit of society, four training companies shared their cyber security awareness and training tactics in this research. In this thesis, we explore how four different training organizations use SETA to foster good cyber security habits, cut down on incidents in information assurance, and boost compliance generally. It may also demonstrate how training organizations are addressing a range of challenges, thereby contributing to a greater public understanding of the challenges inherent in SETA programme design and implementation.

7.4. Recommendations

Information technology (IT) managers in companies all over the world can use the methods uncovered by this research to improve their SETA program implementation. The purpose of this research was to investigate the strategies employed by IT executives in the hospitality sector to establish and maintain a functional SETA. The results of this study demonstrate how three crucial strategies can be applied to the creation of a SETA program to protect computer science data and information systems. The first step toward being so ready was providing people with relevant, consistent, and ongoing education about cyber security. The second was education about potential dangers and weaknesses. The last phase involved sharing the findings and anticipated outcomes.

One piece of advice for CS IT leaders is to conduct a comprehensive strategic, operational, and tactical review of the current SETA program implementation involving all relevant stakeholders. Every member of the organization is responsible for maintaining the integrity of the business's computer networks and data. Key stakeholders must analyse the current threat landscape and future trends in cyber security to develop an effective SETA strategy. IT managers at hospitality companies should either pay for a subscription to a service that provides threat intelligence or assemble this data independently. IT managers in the hospitality sector should routinely review data on cyber threats to better target security education and awareness initiatives. As such, this thesis should serve as a helpful reminder of the advantages of adopting a SETA program for those CS who have yet to do so.

Second, the report recommends that CS IT leaders critically examine the methods they are currently employing to implement the SETA program.

IT managers should also take stock of their staff's knowledge of information security. According to the findings, it is essential to implement continuous, persistent, and relevant cyber security awareness and training to foster the desired behaviour. CIOs from all sectors should pool their resources and work together to disseminate their best SETA practices. Through teamwork, IT leaders can stand by one another against organized, well-funded criminals. Effective SETA practices that reinforce desired behaviour and lessen the likelihood of accidental insider threats can be rapidly disseminated through collaborative efforts and the exchange of good SETA strategies.

An additional piece of advice is to review existing policies and procedures to check if employees are abusing the company's information systems. As part of this policy review, it is important to look at how well schools are following the guidelines set out in the policy and

how they are handling corrective training. Leaders in IT must foster a climate where employees know what is expected of them from day one and how they will be measured throughout their tenure. To ensure compliance, workers need to be made aware of the expected outcomes and the expectations that will shape their behaviour.

Our final piece of advice for IT leaders in CS is to investigate the social cyber sub-domain so that their SETA projects can benefit from the findings in psychology, sociology, and human behaviour. The success of efforts to raise cyber security awareness and educate the public is largely dependent on the efforts of individuals. IT managers can learn a lot about human nature by implementing strategies that motivate their CS to act in a morally commendable fashion. IT managers should think about getting psychological evaluations of their staff so they can better understand their employees and encourage good behaviour. IT managers need to study sociology and social psychology to learn how to create a culture that fosters good cyber security practices and a climate that motivates employees to act ethically online.

7.5. Proposals for Further Research

Several issues call for further investigation. An initial problem with the study was that there wasn't a huge number of CS to evaluate. A larger sample size and a broader selection of businesses could be examined in future studies. The participation of IT industry leaders who provided data and information in line with the existing literature was crucial to the success of this study. It's worth noting that different CS and different people might turn up new insights that add to what we already know.

Participants may have lied or omitted information for various reasons, which is another limitation of this study. From what I could tell, everyone gave honest answers and made it clear when they didn't know something or weren't allowed to share confidential information. Possible future solutions to the problem of open disclosure in the field of organizational cyber security practices include the use of anonymous surveys for data collection.

An interesting and potentially useful area of research would be to examine SETA programs from the perspective of workers. Understanding how the SETA program has been successful and how employees' families have been affected by cyber security education would be very interesting. The themes that were most significant to them as individuals would also be fascinating to investigate.

There is room for more research into the field of information security, and it could be fruitful to look at cyber security from the perspectives of industrial/organisational, social, and

behavioural psychology. It would be instructive to gain insight into the processes by which businesses foster positive cyber security cultures and encourage desired behaviours by means of symbols, norms, and ideals. It would also be interesting to look at how and why workers react to workplace information security policies, legislation, and consequences. A related area of study would be to examine whether there is a correlation between the big-five personality traits of openness, conscientiousness, extraversion, agreeableness, and neuroticism and cyber security behaviour. A more complete picture of the characteristics that define and motivate cyber security actions could help inform CS practices.

7.6. Reflections

Doing well in a doctoral program requires a lot of perseverance, patience, and determination. Although I had known that earning a Ph.D. and working as a professor was on my list since my third year of college, I never felt prepared to take on the rigorous coursework and lengthy hours required to graduate. I considered the fact that I had other commitments and was lacking the prerequisites for a Ph.D. Over the course of my twelve years of active duty, I underwent a profound personal transformation. Since then, I decided to pursue my Ph.D. in the field.

When I first started out, I did not understand the value of things like compound interest and ongoing improvement. Developing a research topic, writing a detailed academic thesis, and gathering data have all been beneficial to my personal, professional, and academic growth.

My research and writing skills, as well as my understanding of my field, have all been enhanced by my time spent earning a doctorate. It has also helped me become much more tenacious, resilient, and patient. Throughout the course of this journey, I have been faced with a number of challenges that have tested my resolve and determination to give up. Because of my wife's support, I was able to achieve success. Her unwavering confidence in me and words of encouragement were instrumental in my finishing the project. After finishing my master's degree, I was on the verge of giving up, but persistence and honesty with a reliable confidant kept me going. I cannot stress enough the importance of having people who will encourage you and encourage you to keep going when you are in the midst of this massive effort that is a Ph.D.

REFERENCE - Digital

Barab, S. & Squire, B. (2004). Design-based research: Putting a stake in the ground. Journal of the Learning Sciences, 13(1): 1-14. Available online at http://website.education.wisc.edu/kdsquire/manuscripts/jls-barab-squire-design.pdf

Bicak, A., Liu, X., & Murphy, D. (2015). Cybersecurity Curriculum Development: Introducing Specialties in a Graduate Program. Information Systems Education Journal, 13(3) page 99-110. http://isedj.org/2015-13/ ISSN: 1545-679X

Burchell, J. (2009). The legal protection of privacy in South Africa: A transplantable hybrid. Electronic Journal of Comparative Law, 13(1), page 1-26. Retrieved from http://www.ejcl.org/131/art131-2.pdf

Chertoff, M. (2008). The cyber security challenge. Regulation & Governance, 2(4), page 480-484. https://doi.org/10.1111/j.1748-5991.2008.00051.x

Chickowski, E. (2013). Top 15 Indicators of Compromise. Dark Reading. Retrieved from http://www.darkreading.com/ attacks-breaches/top-15-indicators-of-compromise/d/d-id/1140647?

Choo, K. R. (2018). 'The Cyber Threat Landscape: Challenges and Future Research Directions.' Computers & Security.30: page 719- 731

Cisco. (2017). Annual cyber security report. San Jose, CA. Retrieved from http://www.cisco.com/c/en/us/products/security/security-reports.html

Cloete, F. (2012). E-government lessons from South Africa 2001-2011: Institutions, state of progress and measurement. The African Journal of Information and Communication (AJIC), 12, page 128-142. https://doi.org/10.23962/10539/19712

Department of Telecommunications and Postal Services (DTPS). (2016). National Integrated ICT Policy White Paper. Government Gazette, 176(40325). Retrieved from http://www.gov.za/sites/www.gov.za/files/40325_gon1212.pdf

Design-Based Research Collective. (2003). Design-based research: An emerging paradigm for educational inquiry. Educational Researcher, 32(1): page 5-8.

Donovan, K. P. (2015). The biometric imaginary: Bureaucratic technopolitics in post apartheid welfare. Journal of Southern African Studies, 41(4), page 815-833. https://doi.org/10.1080/03057070.2015.1049485

Enosh**,** G., Tzafrir, S. S., & Stolovy, T. (2014). The development of client violence questionnaire (CVQ). *Journal of Mixed Methods Research*, *9*(3), 273–290. https://doi.org/10.1177/1558689814525263

Fripp, C. (2016). Anonymous begins #OpAfrica: Claims thousands of SA sites compromised. Retrieved from http://www.htxt.co.za/2016/02/12/ anonymous-makes-good-on-promise-goes-after-sa-government-websites/

International Telecommunication Union (ITU) World Telecommunication. (2016). ICT Indicators database. Available online at http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

IT Web (2023). Cyber crime's annual impact on SA estimated art R2.2 billion. Available online at ttp://www.itweb.co.za/content

Johnson, R. B.B. & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come.
Educational Researcher, *33*(7), 14–26. https://doi.org/10.3102/0013189X033007014

Karspesky Labs. (2017). Cybersecurity Awareness, www.karspesky.com

Kirlidog, M., Van der Vyver, C., Zeeman, M., & Coetzee, W. (2016). Unfulfilled need, Reasons for insufficient ICT skills in South Africa. Information Development, page 1-15 https://doi.org/10.1177/0266666916671984

KPMG Global Cyberecurity Task Team (2022), Africa Cyber Security Outlook, http://www.kpmg.com

Lewis, J. A. 2015. 'National Perceptions of Cyber Threats'. Strategic Analysis. 38 (4): page 566-576. Internet: http://dx.doi.org/10.1080/09700161.2014.918445 Accessed 20 September 2018.

Maxwell, J. A. (2016). Expanding the history and range of mixed methods research. *Journal of Mixed Methods Research*,
10(1), 12–27. https://doi.org/10.1177/1558689815571132

McGettrick, A. (2013). Toward Curricular Guidelines for Cybersecurity. Report of a Workshop on Cybersecurity Education and Training. Retrieved from http://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf

McGettrick, A. (2013). Toward Curricular Guidelines for Cybersecurity. Report of a Workshop on Cybersecurity Education and Training. Retrieved from http://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf

Morgan, S (2003) Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021, https://www.csoonline.com/

Mutula, S. M., & Mostert, J. (2010). Challenges and opportunities of e-government in South Africa. The Electronic Library, 28(1), page 38-53.
https://doi.org/10.1108/02640471011023360

National Planning Commission, National Development Plan Vision (2030), Chapter 9, page 259, www.nationalplanningcommission.org.za

Council. htxt.africa. Retrieved from http://www.htxt.co.za/2013/10/16/whos-whoon- south-africas-new-cyber-security-advisory-council

Peekhaus, W. (2014). South Africa's Promotion of Access to Information Act: An analysis of relevant jurisprudence. Journal of Information Policy, 4, page 570-596.
https://doi.org/10.5325/jinfopoli.4.2014

Poth**,** C., & Munce, S. E. P. (2020). Commentary—Preparing today's researchers for a yet unknown tomorrow: Promising practices for a synergistic and sustainable mentoring approach to mixed methods research learning. *International Journal of Multiple Research Approaches, 12*(1), 56-64. doi:10.29034/ijmra.v12n1commentary

Pricewaterhouse Coopers (PWC) (2015). Report on Managing Cyber Security Risks in an Inter-connected work. Cyber security industry outlook, p5, www.pwc.com/sg

State Security Agency (SSA) (2015). The National Cybersecurity Policy Framework (NCPF). Government Gazette (39475). Retrieved from https://www.gov.za/sites/www.gov.za/ files/39475_gon609.pdf

Technopedia (2010). Technopedia Dictionary (Networking), https://www.techopedia.com/definition/2493/cyberspace

Tehan, R. (2015). Cybersecurity: Authoritative Reports and Resources, by Topic. Congressional Research Service, April 28. As of 12 October 2015: https://www.fas.org/sgp/crs/misc/R42507.pdf

Turok, B. (2017). South Africa's lopsided economy. New Agenda: South African Journal of Social and Economic Policy, 2017(65), page 6-9. Retrieved from http://hdl.handle.net/10520/ EJC-900a1510b

Van Heerden, R., Von Soms, S., & Mooi, R. (2016). Classification of cyber-attacks in South Africa. In IEEE (Ed.), IST-Africa Week Conference. New York: IEEE. https://doi.org/10.1109/ISTAFRICA.2016.7530663

Association (Ed.), Cyber behaviour: concepts, methodologies, tools, and applications (page 1583-1597). Hershey: IGI Global. https://doi.org/10.4018/978-1-4666-5942-1.ch082

Volz, D., & Shepardson, D. (2017) Criticism of Equifax data breach response mounts, shares tumble. Reuters. Retrieved from https://www.reuters.com/article/usequifax- cyber/criticism-of-equifax-data-breach-response-mounts-shares-tumbleidUSKCN1BJ1NF

Wolfpack. (2013). The South African cyber threat barometer. Johannesburg. Retrieved from http://us-cdn.creamermedia.co.za/assets/articles/attachments/41981_ sa_2012_cyber_threat_barometer_medium_res.pdf

World Economic Forum (2023), Future of Jobs - Insight Report (page 24). http://http.weforum.org

Wicks, D. & Sallee, J. (2016). Transactional distance or Community of Inquiry: A need for a theory of focus in online learning. Russian-American Education Forum. Available online at http://www.rus-ameeduforum.com/content/en/?task=1000864&iid=10

REFERENCES – Non-Digital

Abraham, S., Chengalur-Smith, I. (2011). The Role of Conflict Resolution in Designing and Implementing Information Security Policies: An Institutional Perspective. Proceedings of AMCIS (America's Conference on Information Systems), Detroit, MI.

Amiel, T. & Reeves, T.C. (2008). Design-based research and educational technology: Rethinking technology and the research agenda. Educational Technology & Society, 11(4): 29-40.

Anema, I. (2014). Integrative Learning and Evidence-Based Practice: Mastering the Process. Contemporary Issues in Communication Science and Disorders. (41). 1-11.

Archer, M (1998). 'Realism and morphogenesis' in Archer et. al. In Margaret Scotford Archer (ed.), Critical Realism: Essential Readings. Routledge.

Assante, M. J., Tobey, D.H. (2011). Enhancing the cyber security workforce, IEEE IT Professional, (13). Page 12–15.

Baldwin, D.A. (1997). 'The Concept of Security'. Review of International Studies. 23(1): page 5-26.

Bajaj, K. (2010). The Cyber Security Agenda – Mobilizing for International Action. New York, East West Institute.

Ben Dipietro, (2017) Cyber Education: A Multi-Level, Multi-Discipline Approach, Wall Street Journal,

Bishop, M. (2010) "Academia and Education in Information Security: Four Years Later," Fourth National Colloquium on Information System Security Education

Bishop, M.& Irvine, C. (2010). Demystifying Cybersecurity. IEEE Computer and Reliable Societies. May/June 2010

Bourne, M. (2014). Understanding Security. London. Palgrave Macmillan.

Border, C., & Holden, E. (2003). Security education within the IT curriculum. CITC.

Brechbhl, H. Bruce, R. Dynes, S. & Johnson, E. M. (2010). 'Protecting Critical Information Infrastructure: Developing Cybersecurity Policy'. Information Technology for Development. 16 (1): page 83- 91.

Cleary, B. (2008). How safe is your data? Strategic Finance, 90(4), page 33-37.

Buzan, B. (1998). People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era. 2nd edition. New York: L. Rienner Publishers. London

Caldwell, T. (2013). Plugging the cyber-security skills gap. Computer Fraud and Security, July 2013.

Cavelty M. (2010) Cyber-Security and Threat Politics. CSS Studies in Security and International Relations. Routledge, London, New York

Dunn Cavelty & Myriam (2008) Cyber-Security and Threat Politics, London, New York: Routledge.

Chandarman, R. (2016). Cybersecurity awareness of students at a private higher education institute in South Africa. Master's dissertation, University of KwaZulu-Natal, Westville, Durban

Cooper, D., & Schindler, P. (2008). Business research methods (10th ed.). New York, McGraw-Hill/Irwin.

Creswell, J. W. (2010). Designing and conducting mixed methods research. Thousand Oaks: Sage

Creswell, J.W. (2013). Research design: Qualitative, quantitative and mixed methods approaches. (2nd Ed.) Thousand Oaks, California: Sage.

Crowley, Ed. (2003). Information system security curricula development, page 249-255. 10.1145/947121.947178.

Endicott-Popovsky, Barbara & Popovsky & Viatcheslav. (2014). Application of pedagogical fundamentals for the holistic development of cyber security professionals. ACM Inroads. page 57-68.

Forcht, K.A. (1986). Computer Security Management, Boyd & Fraser, Danvers, MA.

Fourie, L (2014). Abdolhossein Sarrafzadeh, Shaoning Pang, Tamsin Kingston, Hinne Hettema & Paul Watters; The Global Cyber Security Workforce – An Ongoing Human Capital Crisis

Friedman A.A. & West, D.M (2010). Privacy and Security in Cloud Computing. The Center for Technology Innovation.

Garrison, D.R., Anderson, T. & Archer, W. (2003). A theory of critical inquiry in online distance education. Handbook of distance education, (page 113-127). In: M. Moore (Ed.), Handbook of distance education. New York: Erlbaum.

George, D. & Mallery, P. (2013). SPSS for Windows step by step: A simple guide and reference. 11.0 update (4th ed.). Boston, MA: Allyn & Bacon.

Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. European Journal of Information Systems, 2: page 135-146.

Hair, J., Black, W., Babin, B., Anderson, R., & Tatham, R. (2006). Multivariate data analysis (6th ed.). Uppersaddle River, N.J.: Pearson Prentice Hall.

Holmberg, B. (1986). A discipline of distance education. International Journal of E-Learning & Distance Education, 1(1): page 25-40.

Hsu, C. & Backhouse, J. (2002). Information systems security education: Redressing the balance of theory and practice. Journal of Information Systems Education, 13(3), page 211-218.

Irvine, C., Chin, S.K. & Fruickle, D. (2018). Integrating security into the curriculum. Computer, 31(12), page 25-30.

Johnson, R. W. (2017). How long will South Africa survive? The crisis continues. Johannesburg: Jonathan Ball.

Kvale, S. & Brinkmann, S. (2009). Interviews: Learning the craft of qualitative research interviewing. Los Angeles: Sage

Kapoor, N.F. (2017). Capabilities, technologies, and firm exit during industry shakeout: Evidence from the global solar photovoltaic industry. Strategic Management Journal (2018) 39(1) page 33-61

Kemmerer, R. (2003). Cybersecurity. SIGCSE Bulletin. 35. Page 705- 715. 10.1109/ICSE.2003.1201257.

Kizza, J. M. (2014). Computer Network Security and Cyber Ethics, Fourth Edition. Jefferson, NC: McFarland &Co Inc. Kvale, S., & Brinkmann, S. (2009). InterViews: Learning the craft of qualitative research interviewing (2nd ed.). Thousand Oaks, CA, US: Sage Publications, Inc.

Leedy, P.D. & Ormrod, J.E. (2010). Practical research planning and design. 9th edition. Upper Saddle River, NJ: Merrill Prentice Hall.

LeClair, J., Abraham, S. & Shih, L. (2013). An Interdisciplinary Approach to Educating an Effective Cybersecurity Workforce. Proceedings of the on InfoSecCD' 13 Information Security Curriculum Development Conference

Locasto, E. M., Ghosh, K. A., Jajodia & S., Stavrou, A. (2011). Virtual Extension The Ephemeral Legion: Producing an Expert Cyber-Security Work Force from Thin Air, Communications of the ACM. 54 (1) page 129-131.

Martini, B., & Choo, K. (2014). Building the next generation of cyber security professionals. Proceedings of Twenty Second European Conference on Information Systems, Tel Aviv, 2014. Page 1

Maxwell, J.A. (2012). Qualitative research design: An interactive approach. 2nd edition. Thousand Oaks, CA: Sage.

Mayo, J.& Kearns, P. (1999). A secure unrestricted advanced systems laboratory. In Proceedings of the 30th SIGCSE Technical Symposium on Computer Science Education. New Orleans, USA, page 165–169.

Merriam S,B & Tisdell E.J (2015) Qualitative Research: A Guide to Design and Implementation, John Wiley & Sons. 4th Edition

O'leary, M. (2006). A laboratory-based capstone course in computer security for undergraduates. In Proceedings of the 37th SIGCSE Technical Symposium on Computer Science Education. Houston, Texas USA.

Olson, R. (2016). Chaim Sanders, Comparing Security Curricula and Accreditations to Industry Needs

Oxford, A. (2014). Who's who on South Africa's new Cyber Security Advisory

Paulson, L.D. (2002). Wanted: More network-security graduates and research. IEEE Computer, 35 (2), page 22-24.

Public Safety Canada (2010) Departmental Performance Report. Minister of Public Safety

Remenyi D Williams, B Money, & A Swartz, (2005). Doing Research in Business sand Management, Sage, London

Robson, C. (2012). Real world research: A resource for social-scientists and practitioner-researchers. 3rd edition. Oxford: Blackwell Publishing.

Rowe,D. Lunt, B & Ekstrom J.(2011).The role of cyber-security in information technology education. Proceedings of the 2011 conference on Information technology education - SIGITE '11, 2011

Sandelowski, M. (2000). Focus on research methods: Combining qualitative and quantitative sampling, data collection, and analysis techniques in mixed-method studies. Research in Nursing and Health, 23: page 246-255.

Schneider, W. (2018), "The Development of Metacognitive Knowledge in Children and Adolescents: Major Trends and Implications for Education", Mind, Brain, and Education, Vol. 7/9, pp. page 114-121,

Sobiesk, E., Blair, J., Conti, G., Lanham, M. & Taylor, H. (2015). Cyber Education: A Multi-Level, Multi-Discipline Approach. 10.1145/2808006.2808038.

Thorpe, R., & Holt, R. (2008). The SAGE dictionary of qualitative management research London, : SAGE Publications Ltd doi: 10.4135/9780857020109

Van Vuuren, J. J., Phahlamohlaka, J., Leenen, L., & Zaaiman, J. (2014). An approach to governance of cyber security in South Africa. In Information Resources Management

Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. The African

Werlinger, R. W., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. Information Management & Computer Security, 17(1), page 4-19.

Wiedemann, G. (2013). Opening up to big data: Computer-assisted analysis of textual data in social sciences. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 14(2).

Yang, T, (2001). Computer security and impact on computer science education. Journal of Computing Sciences in Colleges - JCSC.

Yasinsac, A., Erbacher, R.F., Marks, D.G., Politt, M.M., & Sommer, P.M. (2017). Computer forensics education. IEEE Security & Privacy, 1(4), page 15-23.

Yin, R. K. (2009). Case study research: Design and methods (4th Ed.). Thousand Oaks, CA: Sage.

Zohrabi, M. (2013). Mixed Method Research: Instruments, Validity, Reliability and Reporting Findings. Theory and Practice in Language Studies, Vol. 3, No. 2, page 254-262, February 2013

Appendix A : Data Collection Tools

RESEARCH TOOLS

QUESTIONNAIRE

1. **Introduction:**

Hello and thank you for your participation in the survey in advance

The following questionnaire is a part of the study aimed to guide at the development cyber security curriculum within institutes of higher learning in South Africa.

The questionnaire is targeted for Information Technology field academic staff at public and private education institutions.

The questionnaire consists of 22 questions: 16 of them are related to the development of cyber security curriculum/programme in South Africa, 5 questions cover a demographic part. You can either choose answer(s) from suggested options and/or provide your own suggestion. The overall process will take around 10 minutes. The format of the questionnaire ensures confidentiality.

In case of questions or comments please contact

First name	Mduduzi Eric Zakwe
Cell phone	082 662 0597
Email address	64876012@mylifeunisaac.onmicrosoft.com

2. Demographic information:

1. Please indicate your age from the drop-down list:
   a) 1 8 – 24
   b) 25 – 34
   c) 35 – 44
   d) 45 – 54
   e) 55 – 64
   f) 64 +

2. Please indicate your gender from the drop-down list:

a) male
b) female

3. Please indicate how long have you been employed in IT field:

a) <= 1 year
b) 1 year <= 2 years
c) 2 years <= 5 years
d) 5 years <=10 years
e) other:

4. Please indicate how long have you been employed within your company IT filed:

a) <= 1 year
b) 1year <= 2 years
c) 2 years <= 5 years
d) 5 years <=10 years
e) other:

5. Please indicate your current position:

a) Executive / C-level
b) Director
c) Manager
d) System Administrator
e) Network Administrator
f) Technician
g) Other:

1. Which of the cyber security skills do you think are in high demand in South Africa at present?

Information and Network security	
Cryptography	
Secure coding	
Penetration testing	
Digital forensics	
IT Risk and Business continuity management	
Audit	
Legal aspects	
Other:	

2. Which of the cyber security skills do you think will be in high demand in South Africa in 3-5 years?

Information and Network security	
Cryptography	
Secure coding	
Penetration testing	
Digital forensics	
IT Risk and Business continuity management	
Audit	
Legal aspects	
Other:	

3. Cyber security professionals with which cyber security skills do you consider to be difficult to find in South Africa at the present time?

Information and Network security	
Cryptography	
Secure coding	
Penetration testing	
Digital forensics	
IT Risk and Business continuity management	
Audit	
Legal aspects	
Other:	

4. Which cyber security skills are not available for training/education in South Africa at the present time?

Information and Network security	
Cryptography	
Secure coding	
Penetration testing	
Digital forensics	
IT Risk and Business continuity management	
Audit	
Legal aspects	
Other:	

5. Please indicate if any of the directions are taught at your education institution:

Information and Network security	
Cryptography	
Secure coding	
Penetration testing	
Digital forensics	
IT Risk and Business continuity management	
Audit	
Legal aspects	
Other:	

6. Has a company requested from your institution to conduct a cyber security training to raise its employees' cyber security qualification?
   a) Yes
   b) No

7. Has a company expressed interest in higher education programme in cyber security at your education institution?
   c) Yes
   d) No

8. How do you think a company can support development of cyber curriculum in South Africa?
   a) Providing advisory role on cyber security skills initiatives
   b) Working with universities to develop/deliver course content
   c) Employing students on a long-term or short-term internship
   d) Employing students on a long-term or short-term paid internship
   e) Sponsoring master student(s)
   f) Other:

9. Should the Cyber security programme have multidisciplinary approach or should focus on one field?
   a) Focus on one field
   b) Take multidisciplinary approach

10. On which of the directions should the cyber curriculum/ programme focus (choose one or more from the list considering your answer to the previous question)?

Information and Network security	
Cryptography	
Secure coding	
Penetration testing	
Digital forensics	
IT Risk and Business continuity management	
Audit	
Legal aspects	
Other:	

11. How do you think where should the CS programme be established?
   a) State education institution
   b) Private education institution
   c) Military education institution

12. Please select the criteria the academic staff should meet:
    a) Experienced IT professional being employed in cyber security field
    b) Experienced IT professional with higher education in IT field and being employed in cyber security field
    c) Other:

13. Should the cyber curriculum offer employment opportunities to graduate students?
    a) Yes
    b) No

14. Should the cyber curriculum provide internships?
    a) Yes
    b) No

15. Should the cyber curriculum include extracurricular activities (ex. visiting companies on site and observing and/or participating in the actual task accomplishment processes)?
    a) Yes
    b) No

16. Choose one or more criteria you think is important for accepting a student at the CS programme (in addition to the results of the unified national exams)?
    a) Higher education in IT field; at least two years of experience in IT field
    b) Higher education in IT field; experience is not required
    c) Higher education in non-IT field is acceptable; at least two years of experience in IT field
    d) Other:

INTERVIEW GUIDE

Dear Participant:

The overarching aim of the research is to determining the correct state of ICT programmes in relation to cybersecurity in South Africa and develop a cybersecurity framework that can guide the development cyber security curriculum within institutes of higher learning in South Africa.

1. Are there any existing guidelines for cybersecurity education in South Africa that you can share?
2. Does cybersecurity education empower graduates to fight the scourge?
3. How does your institution contribute to building a capable cyber-workforce that can reduce the widening skills gap in the cyber security industry?
4. How do you think cyber curriculum be developed to support a wide- range of security programme /types within the ODL teacher training curriculum?
5. Is there any structure for cybersecurity discipline or a model of curriculum that outlines key dimensions of current industry trends that can be applied?
6. How can the institution support the alignment of academic programs and industry needs in cybersecurity?

Thank you for your time

Appendix B : Ethical Clearance Certificate

UNISA university of south africa

UNISA COLLEGE OF EDUCATION ETHICS REVIEW COMMITTEE

Date: 2021/04/14

Ref: **2021/04/14/64876012/36/AM**
Name: Mr ME Zakwe
Student No.: 64876012

Dear Mr ME Zakwe

Decision: Ethics Approval from 2021/04/14 to 2026/04/14

Researcher(s): Name: Mr ME Zakwe
E-mail address: 64876012@mylifeunisa.ac.za
Telephone: 082 662 0597

Supervisor(s): Name: Prof. SA Ngubane-Mokiwa
E-mail address: mokiwsa@unisa.ac.za
Telephone: 012 337 6188

Title of research:

Developing a framework for effective cybersecurity training in South Africa: The case of the MICT SETA.

Qualification: PhD ODL

Thank you for the application for research ethics clearance by the UNISA College of Education Ethics Review Committee for the above mentioned research. Ethics approval is granted for the period 2021/04/14 to 2026/04/14.

*The **medium risk** application was reviewed by the Ethics Review Committee on 2021/04/14 in compliance with the UNISA Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment.*

The proposed research may now commence with the provisions that:

1. The researcher will ensure that the research project adheres to the relevant guidelines set out in the Unisa Covid-19 position statement on research ethics attached.
2. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

3. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the UNISA College of Education Ethics Review Committee.
4. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
5. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing.
6. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
7. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.
8. No field work activities may continue after the expiry date **2026/04/14.** Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

Note:

The reference number **2021/04/14/64876012/36/AM** *should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.*

Kind regards,

Prof AT Motlhabane
CHAIRPERSON: CEDU RERC
motlhat@unisa.ac.za

Prof PM Sebate
EXECUTIVE DEAN
Sebatpm@unisa.ac.za

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Appendix C: Editors Certificate

Date

CONFIRMATION OF CORRECTIONS

STUDENT NUMBER: .....
CANDIDATE: .....
DEGREE: .....
COLLEGE: Education
FIELD: .....
TITLE: .....

This report confirms that the recommendations from the two/three external examiners were sent to the student in order to effect the changes that were suggested. The student has made the required improvements and I am satisfied that all the suggestions were captured.

Thank you

Yours faithfully

.....
(Supervisor/Promotor)