TOWARDS BUILDING CYBERSECURITY CULTURE IN TVET COLLEGES: IMPACT ASSESSMENT OF BEHAVIOURAL CHANGE STRATEGIES

DUT Research Team

April 2023

ACKNOWLEDGEMENTS

Consider when you have a challenge with your smart device. Who do you go to in your family? That's right, you go to a teenager. They may not even have your iPhone or Samsung, but they figure it out better than you can!

The youth are our digital natives, they have an intuitive ability to relate to modern technology. In the post-pandemic world, they have increasingly become the residential and community go-to people to get ICT help.

It therefore makes sense that to protect the nation we need to educate the residential experts, who are the youth. The TVET system has hundreds of thousands of learners, in all parts of the country. This is the reason we focussed on TVET learners. We believe that this is an innovative model for changing the nations cybersecurity and culture.

"We do not inherit the earth from our ancestors, we borrow it from our children."

The DUT research team comprised Professor Colin Thakur, who is the INSETA Research Chair in Digitalisation, Prof Zoran Mitrovic, an international Cybersecurity consultant, Sudhika Palhad, the Research Manager and Mogandren Govender.

The INSETA team was led by CEO Gugu Mkhize and Research Coordinator, Zakkariya Desai.

The team acknowledges the positive support of INSETAs CEO Ms Gugu Mkhze and DUT's Deputy Vice Chancellor: Research, Innovation and Engagement (RIE) Professor Keo Motaung.

Prof Surendra Thakur

INSETA Research Chair in Digitalisation

Director: Short Course Unit

Durban University of Technology

ABBREVIATIONS AND GLOSSARY OF TERMS

Abbreviation	*Description*
4IR	Fourth Industrial Revolution
Authentication	The process of verifying the identity of a user or device attempting to access a system or network.
Backup	The process of creating a duplicate copy of data or information to protect against data loss due to cyberattacks, natural disasters, or human errors.
Compromises to intellectual property	The unauthorized use, duplication, and distribution of protected IP.
Cyber breach	A security incident in which an attacker successfully gains unauthorized access to sensitive information or systems.
Cyber risk	Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – be it related to individuals, companies, or governments.
Cyber threat	A circumstance or event with the potential to intentionally or unintentionally exploit one or more system vulnerabilities resulting in a loss of confidentiality, integrity, or availability of information or information systems.
Cyberattack	Attempts to damage, disrupt, or gain unauthorised access to a computer, computer system, or electronic communications network. An attack, via cyberspace, targets an enterprise's use of cyberspace to disrupt, disable, destroy, or maliciously control a computing environment or infrastructure; destroy the integrity of the data or steal controlled information.
Cybercrimes Crimes Bill	The Bill deal with offences related to data, messages, computers, and networks involving hacking, the unlawful interception of data, ransomware attacks, cyber forgery and uttering, and cyber extortion. The Bill also grants law enforcement extensive powers to investigate, search, access and seize various articles, such as computers, databases, or networks.
Cybersecurity	The term refers to strategies, policies, and standards encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resilience, and recovery activities, and policies regarding the security of an insurer's operations.

Cybersecurity awareness	Cybersecurity awareness can be seen as a methodology used to educate internet users to be sensitive to the various cyber threats and the vulnerabilities of computers and data to these threats.
Cybersecurity culture	A set of attitudes, behaviours, and practices that prioritise cybersecurity and risk management within an organisation.
Cybersecurity policy	Defines and documents an organisation's statement of intent, principles and approaches to ensure effective management of cybersecurity risks in pursuit of its strategic objectives.
Cybersecurity skills	Cybersecurity skills are a part of e-skills related to skills needed to securely perform business and other operations on the Internet and in the general computer environment.
Cybersecurity strategy	A tool for Program Managers, Authorising Officials (AO) or Authorising Official Designated Representatives (AODR), and relevant review and approval authorities to plan for, identify, assess, mitigate, and manage risks as systems mature.
Data breaches	Security violations in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorised to do so.
Denial-of-Service attacks (DoS)	An attack that is meant to shut down a machine or network, making it inaccessible to its intended users.
Distributed Denial-of-Service attacks (DDoS)	Involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic.
Encryption	The process of converting data into an unreadable format to prevent unauthorized access.
ENISA	The European Union Agency for Cybersecurity.
Firewall	A security system designed to prevent unauthorized access to a network or computer system.
ICT	Information and communication technologies.
Information extortion	Occurs when cybercriminals threaten to disable the operations of a target business or compromise its confidential data unless they receive payment.
Malware	Any type of software designed to harm or disrupt computer systems, networks, or devices.
Password	A secret code is used to authenticate a user's identity and allow access to a computer system or network.
Patch	A software update designed to fix security vulnerabilities in a program or system.
Phishing	A type of social engineering attack that attempts to trick users into giving up sensitive information or downloading malware.
Ransomware	A type of malware that encrypts a user's files and demands a ransom payment in exchange for the decryption key.
Risk assessment	The process of identifying and analysing potential cybersecurity risks and vulnerabilities in a system or network.

Social engineering	A type of cyberattack that relies on human interactions to trick users into revealing sensitive information or performing actions that compromise security.
TVET college	Technical vocational education and training college
Unauthorised disclosure	A communication or physical transfer of classified information to an unauthorized recipient.
Vulnerability	A weakness in a system or network that could be exploited by attackers to gain unauthorized access or cause damage.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

"Anyone who thinks that he can solve the security issues by technology does not understand either security issues or technology issues".

Bruce Schneier, a well-known cryptographer

INSETA AND ITS MANDATE: REFLECTIVE SNAPSHOT

ALIGNMENT TO INSETA RESEARCH AGENDA

It is well-established that cybersecurity is a major risk for insurance companies and employees. It is a risk that affects all types of insurance companies ranging from micro-enterprises to multi-national organisations. Since insurance companies are storing critical personal information and financial data of clients, cybersecurity must be placed at the top of the training and business agenda. As recently argued by an INSETA official, the perilous times of the COVID-19 pandemic, with an increased number of insurance claims, show the utmost importance of cybersecurity in the insurance industry.

On the other hand, INSETA and the Department of Higher Education and Training (DHET) agreed to focus on research and interventions related to TVET colleges. In this regard, this research and intervention entirely fit the above intention.

LINK TO INSETA SKILLS PLANNING

Cyber risks are an inevitable and complex aspect of technology adoption. Cyber risk management is a cornerstone of the safety and security of all kinds of organisations, particularly those in the financial sector.

Within the insurance sector, technology adoption is growing within firms and by clients resulting in both the firm and the clients being exposed to cyber risks. In this regard, cybersecurity risk management takes the idea of real-world risk management in which the human factor plays a major role in making businesses vulnerable. By human factors, we mean TVET colleges management, lecturers, students, and other employees.

Therefore, the need for appropriate awareness, knowledge, and skills training, aimed at the effective implementation of cybersecurity measures through the development of a cybersecurity culture requires a multi-pronged approach. In terms of skills planning, this research adds value as follows:

1. Technological developments have been identified as one of the key drivers of change. The identification of cyber-risks and their mitigation measures are thus important implications for skills planning.

2. Just as complex problem solving, lateral thinking, agility and other competencies are already proven as important skills for both the present time and future workforce. Cybersecurity is also inevitably an emergent core competence (Rewire, 2022).
3. Moreover, as cybersecurity awareness interventions are emphasised in the South African National Cybersecurity Policy Framework (SA Government Gazette, 2015), this research strongly supports this national imperative.
4. In a crisis time such as the COVID-19 pandemic, many organisations used to adapt to working from remote locations, train and equip staff to work under social distancing regulations and enhance cybersecurity (Babuna et al., 2020). Remote working, however, can endanger organisations as the possibilities of cybersecurity breaches substantially increase – particularly for companies not using Virtual Private Networks (VPNs). Hence, there was and still is a need for appropriate cybersecurity awareness and skills training not only for employees in TVET colleges but also for their students. This is particularly true for these often-forgotten youth in rural and peri-urban areas that are attending TVET colleges.
5. Strategic priorities of the INSETA over the Five-year Planning Period 2020-2024 stipulate that the organisation is supporting the public TVET College system. The same Plan advises the implementation of innovative programmes for youth through partnerships with public TVET colleges and employers in the insurance sector.

TVET COLLEGES

BRIEF DESCRIPTION

According to the DHET, these are the main characteristics of TVET colleges:

The Technical and Vocational Education and Training fit into the education system

The South African education system is administered by the Department of Basic Education (DBE) and DHET. The DBE administers school education from Grade R to Grade 12. The DHET administers Post-School Education and Training.

Post-School Education and Training include Universities and Private Higher Education Institutions, TVET Colleges and Private Colleges, newly established Community Education and Training (CET) Colleges, Sector Education and Training Authorities (SETAs), regulatory bodies such as the South African Qualifications Authority (SAQA) and Quality Councils (QCs).

The TVET colleges comprise vocational, occupational and artisan education and training offered by these colleges. Adult Education and Training (AET) is another category of education and training that is offered at both Basic and TVET levels, but it is not usually occupational or vocational by nature. This form of education and training that is usually offered part-time at

Community Learning Centres (formerly known as Adult Learning Centres) is aimed at persons wishing to achieve a national senior certificate.

Community Learning Centres are the campuses of Community Education and Training Colleges. Other programmes offered by Community Education and Training Colleges through the Community Learning Centres include Civic and Voter Education, Small Micro and Medium Enterprise Development and Co-operatives Development, among others.

Figure 1: TVET college environment (source: Majuba TVET College)

TVET as post-school education and training

This band of education and training is also referred to as "post-school", meaning that it refers to education and training that takes place after leaving school, even if only with a Grade 9 completed. The only age restriction for a person wishing to study at the TVET level is that the person should be 16 years or older. The target student group is therefore responsible for senior adolescents and adults who are serious about following an education and training programme to acquire marketable skills.

TVET Colleges cater for the widest range of education and training opportunities at a post-school level

The range of courses on offer at public TVET colleges is very diverse. Some colleges may offer up to 300 different courses. The length of the course and the admission criteria will differ depending on the nature of the course.

TVET COLLEGES AND THE SURROUNDING COMMUNITIES

Community engagement is a broad and wide-reaching concept. It is present in the specialised literature on education but also in so many other fields. For instance, community engagement is mentioned in fields such as power politics and democracy, urban planning, environmental planning and natural resource management, public health or criminal justice research. In each of these contexts, community engagement takes on specific characteristics. Yet, despite all these differences, all strands of community engagement share a common core value, which

is the importance of social involvement in initiatives led by individuals and organisations (UNEVOC, 2019).

Driscoll (2009) maintains that community engagement describes the collaboration between institutions of higher education and their larger communities for the mutually beneficial exchange of knowledge and resources in a context of partnership and reciprocity.

On the other hand, community engagement at the university level can be described as "a distinctive approach to teaching and research that recognises that some learning or discovery outcomes require access to external entities with distinctive knowledge and expertise. The hallmark of engagement is the development of partnerships that ensure a mutually beneficial exchange of knowledge between the university and the community (Holland & Ramaley, 2008:33).

The Kellogg Commission's authors (Kellogg Commission, 1999:10) believe that to be considered 'engaged', institutions must:

- Be able to respond to the current and future needs of students.
- Enrich students' experiences by bringing research and engagement into the curriculum and offering practical opportunities to prepare for life outside of the campus.
- Put their knowledge and expertise to work on the problems faced by the communities they serve.

Based on these definitions, one can generalise by stating that, in higher education (TVET colleges in this case), community engagement rests on the coordinated participation of two sets of stakeholders: (1) the higher learning institution's staff and students and (2) the community (UNEVOC, 2019). Furthermore, higher education institutions should act as leaders and allow for greater technology transfer, more patenting, employment, and commercial outputs (Srinivas & Viljamaa, 2008).

The above plausibly suggests that TVET colleges can positively influence the surrounding communities. This forms a reasonable prediction that an appropriate cybersecurity culture developed at TVET colleges can positively influence the development of the cybersecurity culture of the surrounding communities. More detailed elaboration on this topic is given in Chapter 3, under the section titled "Cybersecurity Culture Overview".

NEEDS FOR THIS STUDY

> "*To effectively deal with cybersecurity, it is prudent that civil society, government, and the private sector play their part in ensuring South Africa has a culture of Cybersecurity. Critical to this is the development of a culture of Cybersecurity, in which the role players understand the risks of surfing in cyberspace*" (SA Government Gazette, 2015).

Technologies cannot solely protect organisations, particularly if incorrectly integrated and utilised. On the other hand, since cybersecurity technologies rapidly advance, most data breaches within organisations are the result of human actors who use and integrate these technologies (Ponemeon, 2012; ENISA, 2018). It is, unfortunately, happening that many times organisations overlook the human factor security depends upon. Hence, technology is often falsely perceived as the immediate answer to cybersecurity problems. However, cybersecurity is primarily a human factors problem, which remains unaddressed (Metalidou et al., 2014; Nobles, 2022).

As humans do themselves pose a threat and vulnerability to the protection of informational resources (Ismail & Yusof, 2018), individuals must also take responsibility for maintaining a secure and vigilant culture at work and, therefore, there is a need to develop and maintain a cybersecurity culture (Reegård et al, 2019).

On the other hand, it is believed by many authors that one of the best ways to capacitate humans is through developing an appropriate cybersecurity culture. Leenen et al (2020) firmly believe that the cultivation of a cybersecurity culture is the best approach to address human behaviour in the cyber domain.

Since people are often the weakest link in an organisation's cybersecurity chain (Teh et al., 2015; De Maggio et al., 2019), organisations of all types (including TVET colleges) should not only provide sufficient cybersecurity training and resources (Chatterjee, 2019) but should also create and maintain a culture of cybersecurity awareness (Norris et al., 2019; Zhan et al/. 2021).

Moreover, the United Nations Economic Commission for Africa proclaimed several years ago that there is a dire need to nurture an information society that exhibits a culture of respecting values, rights, and freedoms in terms of accessing information to build confidence and trust in the use of ICT in Africa (UNECA, 2014). This inevitably includes the development of a cybersecurity culture, which influences a change in mindset, fosters cybersecurity awareness and risk perception and also maintains a close organisational culture, rather than attempting to force secure behaviour (ENISA, 2018).

CYBERSECURITY CULTURE

Cybersecurity Culture (CSC) refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms, and values of people regarding cybersecurity and how they manifest in people's behaviour with information technologies (ENISA, 2018). Cybersecurity culture can also be defined as the shared values, conceptions, attitudes, knowledge and behaviour of individuals and groups focused on creating security (Advenica, 2020).

In this research, we adopt the definition of cybersecurity culture as the promotion of safe cybersecurity practices that integrate seamlessly with people's work and life. It means making people aware of cybersecurity threats and making them amend their behaviour accordingly

to mitigate potential threats. Unfortunately, young people are often less aware of the importance of cybersecurity culture (Lewis, 2020), which justified this study aimed at building cybersecurity culture in TVET colleges. Strong and healthy cybersecurity culture is one where people are knowledgeable about cyber threats, are receptive to technology and process designs, and feel empowered to change their behaviours to help protect themselves and others.

On the global plane, cybersecurity culture addresses major economic, legal, and social issues relating to cybersecurity to help societies to get prepared to face challenges related to the use and misuse of ICT (ITU, 2009). Criminals do not only exploit technical deficiencies but often rely on people to access sensitive data. It is, therefore, the human factor that causes the most serious security breaches. Hence, building and maintaining a strong security culture is an extremely important part of cybersecurity defence (Advenica, 2020).

The literature on cybersecurity culture views culture as something that can be changed and partly managed (Reegård et al., 20190). Many authors argue that knowledge will influence the assumptions, values, and behaviours in the realm of cybersecurity culture (ENISA 2017; Van Niekerk & von Solms 2010). This knowledge can be obtained through raising awareness and conducting (at least) basic cybersecurity training, which forms the crucial part of this research aimed at building a cybersecurity culture in TVET colleges.

Cybersecurity awareness is the main ingredient of cybersecurity culture

Various factors contribute to the lack of cybersecurity awareness in South Africa, for instance, culture, people's attitudes towards technology, and even issues like ignorance (Welaza & Kritzinger, 2019). Others also point out that cybersecurity awareness is one of the major building blocks of a cybersecurity culture. This is confirmed by the International Telecommunication Union by stating that the building blocks of cybersecurity culture are: training awareness, policymakers, justice and police professionals, managers, Information Communication Technology (ICT) professionals, acceptable practices, end-users, and effective cooperation (ITU, 2009).

Cybersecurity awareness frameworks and training are well-established strategies for raising the cybersecurity resilience of people as cybersecurity awareness can be defined as "an ongoing process of learning that is meaningful to recipients and delivers measurable benefits to the organisation from lasting behavioural change" (Dowd, 2016).

The difference between CSC and cybersecurity awareness is that the latter is a single element or sub-set of CSC. People's awareness is only one element of CSC, it takes a broader and deeper view of an individual's cyber security posture, encompassing behaviours, attitudes, norms, beliefs, interactions, etc., as well as awareness (ENISA, 2018).

Although the awareness level of the users positively affects the behaviour, there is still a gap between the user awareness levels and their respective practices and behaviour (Furnell,

2008). This gap can be filled in by an appropriate cybersecurity culture. In other words, for a culture to effectively counter the effects of the human factor, user knowledge (awareness and education) and behaviour need to be addressed (Van Niekerk & Von Solms, 2006). Hence, it can be considered that two of the pillars of cybersecurity culture are awareness and education (Kortjan & Von Solms, 2014). This study is mindful of the importance of these concepts related to the development of cybersecurity culture in TVET colleges in South Africa.

THE ROLE OF TVET COLLEGES IN BUILDING A CYBERSECURITY CULTURE

> "*A professor at a research university receives an email from his college's dean, asking him to download departmental data. The faculty member clicks a link to a page branded with institutional logos and enters his university login. But instead of a download, he's redirected to a webpage that tells him he's been ensnared in a fake spear-phishing effort by the university's cybersecurity office. It alerts the professor that the email could have been a very real scam and offers tips on how to spot such attempts in the future*" (Basinger, 2019).

The Technical and Vocational Education and Training (TVET) colleges are regarded as the cornerstone in addressing unemployment, and poverty and building the economy of South Africa by producing well-equipped artisans. It was predicted back in 2015 that TVET colleges were expected to enrol 2.5 million students by 2030 (Branson et al., 2015).

Faced with the two-pronged challenge of unemployment and acute scarcity of skills and inspired by the arguments for the TVET system, the South African government places great value on its skills development through this system (Zulu & Mutereko, 2020). There are 50 public and 627 Private TVET Colleges which enrolled approximately 789 530 students in 2015 but this was expected to increase to 1 238 000 by 2019 (DHET, 2017). However, the Higher Education Minister Dr Blade Nzimande revealed, in June 2022, that this department has increased the number of students enrolled in TVET colleges from 452 277 in 2020/21 to 580 849 in 2022/23 (Careers Portal, 2022).

To fight the high unemployment rate in the country, and to bridge the inequality gap in various social classes, the government is encouraging learners to consider enrolling with TVET colleges as an alternative to traditional universities. The government wants more young people to attain skills and competencies that will help them find jobs or create their enterprises as artisans.

The TVET colleges can play an important role in enabling young people to pursue better chances for a decent livelihood. However, TVET institutions usually offer a basic set of stereotype courses at low competency levels. These institutions are often poorly equipped, face infrastructural challenges and have difficulties recruiting qualified TVET personnel.

Furthermore, a discrepancy exists in the level of the lecturers and the central need for further training regarding modern technologies. Developmental needs from a teacher's perspective

include the greatest need for development in the content knowledge area of competencies such as new technologies, electronics, and information technology (Zinn, Raisch & Reimann, 2019). This includes the knowledge of cybersecurity as, for example, Social media and digital applications provide new opportunities for social marketing of TVET. This is supported by the fact that most young people readily accept and use mobile communication technology and are active users of social media (Lange, Hofmann & Di Cara, 2020).

Social media campaigns using simple mobile phone applications can be used by TVET institutions and programmes to reach out to groups that are otherwise, with conventional means, not easily reachable. Disadvantaged groups often lack access to relevant information because of mobility restrictions. Social media marketing can address these gaps. However, the interaction via Social Media must be safe and secure – hence the need for cybersecurity training and the development of a cybersecurity culture as the imposters can relatively easily impersonate legitimate users.

Generally, students are getting an increasing understanding of information systems (IS) and information technology (IT) issues, so overall learning strategies devised by course providers must be intrinsically linked with IS/IT strategies to meet student needs now and in the future (Bandara et al, 2014). However, without appropriate cybersecurity practices and culture, these needs might not be achieved.

Another opportunity that ICT offer to TVET colleges is distance learning and e-learning materials that are responsive to the specific needs of target groups. This endeavour also needs to be supported by cybersecurity knowledge, skills, and culture if online teaching and learning are to be beneficial.

Collaborative learning experiences are normally designed and implemented with pedagogical principles very much in mind, whilst security issues are largely ignored. This may lead to undesirable situations that have a detrimental impact on the learning process, its management and learning material (Bandara et al., 2014).

On the other hand, evidence from South Africa suggests that TVET learners are not simply concerned with immediate employability but value other outcomes from their TVET participation, such as respect, active citizenship, and empowerment (Powell & McGrath, 2019). This broadly means that TVET colleges' teachers and students should participate in community engagement. This is a concept that refers to the benefits that people can gain from expanding and developing bonds with each other and resisting the temptation to work in silos (UNEVOC, 2019).

This engagement can also include the building of cybersecurity culture through TVET colleges, which is an indispensable part of the culture in this all-embracing digital era. This is, however, still an inadequately explored area, indicating the need for further exploration. In that regard, it is essential to generate and maintain a positive attitude of TVET teachers, students and

managers towards digital technology and encourage their readiness and ability to use digital teaching and learning methods, and secure teaching and learning material and processes (Bandara et al., 2014; Lange, Hofmann & Di Cara, 2020).

Moreover, students will share high expectations of their e-learning system, in terms of usability, security and protection of their personal information. This could include the secure handling of a student's bank details associated with payments for course fees and other products (Bandara et al, 2014).

The above and similar facts have motivated the need for developing a cybersecurity culture in TVET colleges in South Africa by creating and implementing an appropriate intervention.

THE TASK AT HAND

The challenge with modern ICT is that people are required to be well-equipped in terms of having the necessary IT tools, Internet connectivity and application platforms for various types of internal and external communication. A further challenge for all organisations is to respond to the increased risk of protecting the confidentiality of sensitive information (Bhana, 2020). TVET colleges in South Africa are no exception.

Furthermore, since communities surrounding TVET colleges are rarely empowered to deal with cyber-related threats, this is a weakness that can expose local communities to cyber risks (Grobler et al., 2011). Moreover, unaware, and untrained youth - usual users of modern ICT - can endanger any public or private organisation they digitally interact with.

Given that knowledge and skills have a crucial role in preventing cyber-attacks, prompted the need for an active approach to the matter to speed up cybersecurity awareness and cybersecurity skill acquisition by students and teachers in TVET colleges. In addition, by assessing opportunities to effectively influence building cybersecurity culture in surrounding communities, TVET colleges have come as a very plausible solution.

Young people often lack a sense of control over what is happening in their lives. However, youth will only be able to drive change if they have the sense that they have the power to make a difference. This should be prioritised in youth-centred development strategies in general, (IFAD, 2019) and those related to TVET colleges, in particular. According to many sources cited in this report, secure control over an individual's digital life is possible by developing an effective cybersecurity culture.

It is also crucial to pay attention to the sense of agency. In this study, the agency is seen as an INSETA's role in supporting the awareness and cybersecurity skilling intervention in TVET colleges through supporting the development of cybersecurity culture. At the inception of this study, supported by the preliminary work, it was firmly believed that this endeavour will help youth to advance by safely using digital devices, applications, and services.

However, to achieve the building of a cybersecurity culture in TVET colleges, it is important to appropriately educate TVET teachers and students (managers and other staff also included), which will help to build a cybersecurity culture within the colleges. Hence, appropriate awareness campaigns and cybersecurity-related curricula are seen as the cornerstones for developing a cybersecurity culture in these institutions of higher learning.

PURPOSE AND OUTCOMES OF THE STUDY

The purpose of this research was to obtain a deep understanding of the cybersecurity needs of teachers, students, and managers in TVET colleges and to devise an appropriate awareness and training programme by creating an effective Action plan for building a cybersecurity culture. It was also planned that the Action plan, included in this report, will then be implemented in the selected TVET colleges in the KZN Province.

BENEFITS OF THE RESEARCH

Generally, this two-phased research provides an in-depth analysis of cyber risks associated with various technological advances and relevant cybersecurity measures – particularly focused on the required cybersecurity skills and awareness for TVET students, teachers, and managers.

In its first phase, this Case Study based research provided the foundation for determining the knowledge, skills and behaviour required by the TVET students, teachers, and managers to securely interact using modern ICT. The second phase, based on the Action research approach, will result in the application, monitoring and evaluation of the proposed Action plan. The intervention will be applied to the selected TVET colleges in the KZN: Elangeni and Umfolozi. This phase is planned for the school year of 2023-2024 or later. It was envisaged that this research will bring the following benefits:

TVET colleges

The TVET colleges involved in this research will benefit in the way in which their teachers, students, and managers (including the admin staff) will enhance their own cybersecurity culture thus influencing the enhancement of the cybersecurity culture of the entire institution. It is also envisaged the possibility that the developed cybersecurity culture at the studied institution can influence the development of cybersecurity culture in the surrounding communities, and the communities where students, teachers, and managers live in.

Government

This research can also inform the policymakers regarding the current state of cybersecurity awareness, culture, and skills gaps, at TVET colleges in South Africa. This study also suggests a way of improving the cybersecurity culture at these institutions, which can help policymakers to devise appropriate measures for enhancing cybersecurity posture through developing a cybersecurity culture.

INSETA

INSETA will contribute to the development of skills related to the cybersecurity culture in TVET colleges as well as to the awareness campaigns at these institutions. Furthermore, the recommendations coming from this study can be emulated by other TVET colleges and other organisations, including INSETA.

There is also another opportunity, which is a “missing market” that is claimed to be lying dormant, ignored by corporations, yet worthy of attention for its potential to contribute to both economic and social prosperity – it is the Bottom of the Pyramid Market (Prahalad and Hammond, 2002). This possibly presents a good opportunity for insurance companies to engage with the communities surrounding TVET colleges. Furthermore, some teachers or students might even become insurance intermediaries for which cybersecurity training will be inevitable.

CHAPTER 2: A GENERAL OVERVIEW OF CYBERSECURITY

AN OVERVIEW OF CYBERSECURITY

In many nations across the globe, cybersecurity is accepted as a national priority (CSIS, 2011; CISA, 2022). However, to understand the concept of cybersecurity, it is important to grasp the notion of cyberspace, which is a human-made information environment created where computer-related telecommunication equipment and other components allow fast movement of large amounts of data (Williams, 2014).

Many of the objects and identities that exist within cyberspace are nonphysical. The terrain includes objects such as radio waves, cell phones, fibre optic cables, satellites, laser beams, software, firmware, and anything that can be linked together to create a digital network (Magee, 2013). The Internet is the most notable network that resides in cyberspace.

Consequently, the landscape of cybersecurity is large, ranging from individuals and organisations to nations, and continuously evolves with new threats and countermeasures. This dynamic nature of cybersecurity makes it challenging to find an objective consensus even on a definition (Kavak et al., 2021).

The Collins English Dictionary (2020) sees cybersecurity as the state of being safe from electronic crime and the measures taken to achieve this while Kaspersky (2018) define cybersecurity as the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

Kavak et al (2021) characterise cybersecurity along three dimensions: targets, threats, and preventive measures. These dimensions were inferred from the literature review and structured as a characterisation of cybersecurity. The purpose of the definition and its characterisation is to provide a foundational understanding of the different relevant components of cybersecurity and the areas in which simulation and modelling can aid cybersecurity.

Targets refer to systems, data, and personnel of interests whose breach or access can provide benefits to non-legitimate users or parties. These targets are categorised as Information and Communications Technology (ICT), data systems, and human systems (i.e., personnel).

Threats refer to “any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), organisational assets, individuals, other organisations, or the nation through an information system via unauthorised access, destruction, disclosure, modification of information, and denial of service” (Kissel, 2013).

The best cybersecurity defence is the one that stops attacks from ever occurring. It is almost impossible to achieve as long as systems remain connected to other systems via networks or

the Internet. Therefore, Kavak et al (2021) rely on preventive measures which we categorize into three areas: technology, education, and policy.

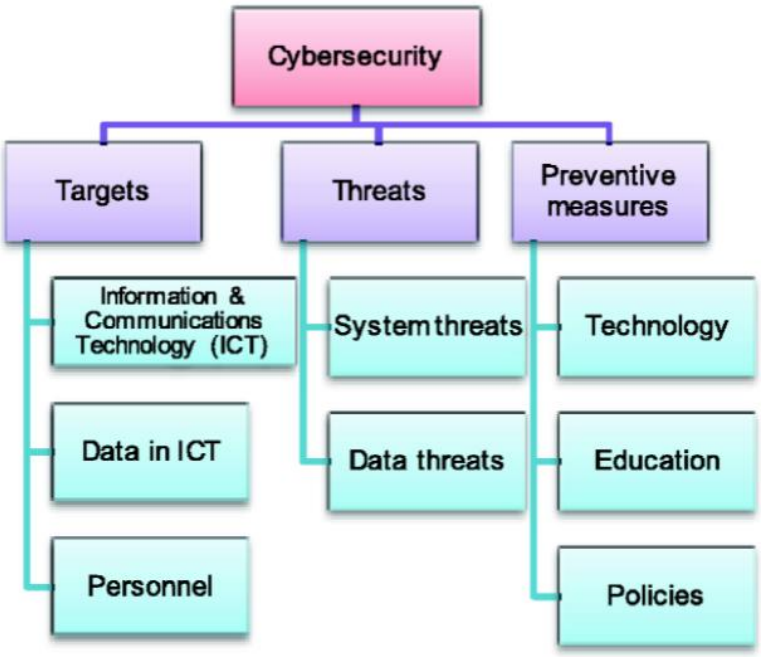

Figure 2: Characterisation of cybersecurity (source: Kavak et al., 2021)

Technology encompasses the tools, techniques, and software that detect, prevent, or stop an attack. A few of the common technologies include anti-virus software, firewalls, and automated updates.

Education occurs through the implementation and enforcement of "policy and procedures." With cyberspace being such a critical component of almost all organisations, it is necessary to describe acceptable uses and responsibilities, explicitly. This type of preventative measure is, understandably, one of the key themes in this research related to TVET colleges.

Documented best practices and formal **policies** shared throughout organisations can aid users and improve security. Additionally, governments should craft laws and determine enforcement protocols for cyberattacks.

Due to a growing understanding that cybersecurity needs to be addressed also through organisational measures (in the above definition: education and policy) and not by technical measures alone, cybersecurity culture is attracting increasing attention (Reegård et al., 2019). Furthermore, cyberspace is categorised into three layers: physical, logical, and social (Kabanda, 2018), hence this study is accordingly concerned with the social level to which cybersecurity culture is related.

THE GENERAL TREND OF CYBER-ATTACKS

With the adoption of digital technologies, cyber-attacks are on the increase, and it is likely to grow in the coming years. With more connectivity and less isolation from the outside world,

the risk of cyber-attacks is high, and the number of cybersecurity incidents continues to increase (NSM, 2018; Online Trust Alliance, 2018). As we have witnessed, this is particularly true at times of a stagnant worldwide economy (caused, among other factors, by the COVID-19 pandemic), which pushes for increased productivity and reduced costs, increasingly realised through the deployment of modern ICT.

Modernising the economy and ICT infrastructure, however, multiplies the possibility of cybercrime activities. The average cost of a cyber-attack in 2019 rose to between USD 108k to USD 1.4bn (depending on the business size), while the average global spend on security products and services is estimated at a new high of USD 124 bn (Kaspersky, 2020). Data breach costs South African companies an average of R40.2 million in 2020 (IOL, 2020).

In July 2022, IBM Security released the annual Cost of a Data Breach Report, revealing costlier and higher-impact data breaches than ever before, with the average cost of a data breach in South Africa reaching an all-time high of R49.25 million for surveyed organisations. With breach costs increasing nearly 20% over the last two years of the report, the findings suggest that security incidents became more costly and harder to contain compared to the year prior (IBM, 2022).

More targeted ransomware, the variety of phishing attacks, the evolution of mobile malware attacks, and risky business with IoT devices are some of the most notable cybersecurity trends in the last two years. Smart consumer devices are spreading faster than they can be secured. The trend of an increasing number of connected devices and the lack of awareness and user skills causes uncontrolled access to personal data, which could severely destabilise the digital society of any company.

On the global plane, political and economic divisions between East and West also lead to increased security threats from outside of countries' borders. Africa has one of the highest cybercrime cases, resulting in considerable financial losses. Despite this, the citizens in African countries are barely educated on cyber risks and awareness campaigns are non-existent (Bada et al., 2019).

With many organisations already keeping more of their staff working from home, the insider threat will become even more pressing. The data breach-related financial cyber-threats are up there with the worst of them, notably because they usually end with a direct monetary loss. According to a report from IBM and the Ponemon Institute, the average cost of a data breach in 2020 amounts to USD 3.86 million. In 2022, the average data breach cost reached a record USD 4.4 million (CNET, 2022). Hence, it seems that cybersecurity challenges are here to stay, at least in the foreseeable future.

CYBER-ATTACKS ON THE HIGHER EDUCATION INSTITUTIONS

FACTORS THAT MAKE HIGHER EDUCATION A PRIME TARGET FOR CYBERCRIMINALS

Building a more resilient higher education institution that can bounce back from cyber events quickly is based on recognising that it is no longer a matter of if these events will occur, but when. This Deloitte's (2018) statement is accompanied by a list of factors that make higher education a prime target for cybercriminals:

- **Wide variety of valuable data**: Institutions of higher learning have sensitive data about students, parents, alumni, faculty, and staff. Records are routinely retained decades after students have graduated from an institution. Furthermore, colleges and universities, particularly those that engage in high volumes of research, often house proprietary data from a wide range of corporations and government entities. The vast volume of potentially valuable data housed at most institutions of higher learning tends to make them highly attractive targets.
- **Lack of centralised structure**: Institutions tend to house their sensitive data in many different locations rather than one centralised hub. Student data may be kept in a variety of other locations: alumni offices, central administration, or even at the department level for graduate programs. This decentralised structure can give cybercriminals a wide range of paths to exploit vulnerabilities in the disparate systems that house sensitive data.
- **Organisational vulnerabilities**: The decentralised nature of data storage in institutions of higher education is often paralleled by similar organisational and structural issues. The responsibility for implementing security measures and determining processes may lie with several different stakeholders in a wide range of departments. Deloitte's (2018) report suggests that institutions generally lack a top-down command structure that makes new safeguards easy to implement. Consequently, departments, individual professors, or students may be slow to engage in the practices necessary to improve cybersecurity.
- **Widespread use of personal devices**: Administrators, faculty, and staff are often unaware of the extent to which they may be exposing their institution to cyber risks when they download sensitive data to less well-protected personal devices. As a result, even if an institution has robust security measures in place, any number of individuals at the institution may, through carelessness or unintentionally, through lack of awareness, expose sensitive data.

The report by Collegis Education (2021) adds to this list the following:

- **Open access**: College campuses are designed to be accessible, allowing information to be freely shared - meaning that schools have their doors open: both physically and digitally.
- **Remote operations**: Students and staff may increasingly be using insecure wireless networks to connect remotely. Also, digital connections can allow people to be more easily tricked.

- **Research**: Attackers are often drawn to the sensitive nature of research on intellectual property.
- **Outdated systems**: Many schools are still using legacy technology systems that can be easily exploited.
- **Large, untrained user networks**: Schools have many users who lack security awareness and can unknowingly admit malware onto their networks through their devices or applications.

The business risks associated with a breach can range from financial and reputational impact to the ability of an institution to carry out its mission (Deloitte, 2018; Colleges Education, 2021):

- **Financial impact** as the sheer financial cost of a breach can be significant.
- **Impact on operations** since virtually every facet of the modern school depends to some extent on properly functioning technology. A significant data breach can be crippling to the daily operations of a university.
- **Reputational damage** with **consumers, corporate partners,** and **government agencies** as corporations are less likely to be interested in partnerships with universities whose research data has been breached. The same holds for institutions that seem to lack a clear, strong resilience plan and set of processes for dealing with cyber threats.
- **Operational**: Ransomware attacks can prevent students, staff, and faculties from accessing key learning and financial systems, bringing educational and business operations to a halt.

CYBERSECURITY IN EDUCATION WARRING STATS

Cybersecurity in education is a topic that has been raised in profile over the last few years, partly because of the increasing number of attacks, particularly during the onset of the coronavirus pandemic. Also, among all sectors in 2021, higher education had the slowest recovery times following an attack (Sophos, 2022). Hence, cybersecurity in education must be taken more seriously. The following stats support this viewpoint (Impact, 2021):

Many incidents in few recent years

The stats show that there have been over one thousand incidents in the last four years alone. These incidents include:

- Unauthorised disclosures, breaches or hacks resulting in the disclosure of personal data.
- Ransomware attacks.
- Phishing attacks result in the disclosure of personal data.
- Denial-of-service attacks.
- Other cyber incidents resulted in school disruptions and unauthorized disclosures.

In 2019, there were reported 348 incidents, nearly three times as many as in 2018 and 2020, this figure rose further to 377. It is estimated that this trend will continue.

Inadequate current security of the data centre

Some 96% of IT decision-makers believe their organisations are susceptible to external cyberattacks and 71% say they are not prepared to cope with them (Webroot, 2017). Concerning education organisations, the information they possess is extremely sensitive, and it is simply not viable to safeguard it in a server that does not have the protections afforded to the highly rated data centres. This was still commonplace in 2021 and 2022.

Higher learning institutions are the second uppermost target for ransomware attacks

Ransomware in 2020 has increased by a factor of seven compared to 2019. Usually, victims of such attacks are in a “lose-lose” situation: if the ransom is paid, then the money is lost, and cyber criminals are encouraged to pursue further attacks. If the ransom is not paid, organisations have to face the prospect of having their data leaked. Colleges and universities worldwide experienced a surge in ransomware attacks in 2021, and those attacks had significant operational and financial costs (Sophos, 2022).

Circumventing cybersecurity protection by students or staff

As it is important to implement the relevant cybersecurity technologies in educational institutions, it is also important for them to carry out policies on campus that encourage safe cybersecurity practices. However, Webroot's (2017) research shows that 42% of schools have students or staff that circumvent cybersecurity protections. According to the newest reports, students and institutions are notoriously famous for their lack of concern with cybersecurity (IvyPanda, 2022).

Social engineering attacks in Higher education

Cyberattacks rely on human error to succeed. They work based on a law of averages approach, determining that if they target a set number of victims, they will be successful in their attempts. According to Verizon's 2022 Data Breaches Investigations Report, 82% of data breaches involved a human element (Verizon, 2022).

This is frequently happening through Social Engineering, which involves manipulating victims into giving up sensitive information to a third party. This is often achieved by impersonating a trusted friend, colleague, or organisation associated with the target.

Consequently, human error is the number one cause of data breaches from cyberattacks, with 52% of incidents directly attributable to them. Therefore, no wonder that 41% of higher education cybersecurity incidents and breaches were caused by Social Engineering attacks (Impact, 2019).

Phishing emails

The proportion of users in education who have fallen for phishing attacks is considerable. Besides, the number of people who fall for these kinds of attacks is indicative of both how prevalent and how successful this type of cybercrime is. On average, 30% of users in the education industry have fallen for phishing emails in the last several years.

Price of educational records on the black market

Educational records and healthcare records are some of the most sought-after data for cybercriminals. These sectors provide extremely high levels of financial gain for hackers. Educational records could fetch up to USD 265 on the black market in 2020. When considering that the going rate for a credit card is just over USD 5, it comes as no surprise that education and healthcare organisations are being targeted to the extent they currently are.

A huge number of cyberattacks in educational institutions

Most education organisations have been the victim of a cyberattack. This mostly concurs with the rapid rise of attacks seen over the last several years and should serve as a warning to administrators. Some 87% of educational establishments have experienced at least one successful cyberattack (RSA Conference, 2017). However, a few years back, 73% of organisations are unprepared for cyberattacks and many of them remain unprepared even after an attack (Inc, 2018).

A recent Check Point report (Check Point, 2021) warned that not much is changed as 2021 recorded a record-breaking number of cyberattacks, with a 50% increase in overall attacks per week on corporate networks compared to the year before. Cybersecurity researchers have recorded millions of cyberattacks per hour attempting to exploit Internet vulnerabilities, calling it a “cyberattack pandemic”.

In October 2021, it was verified a 40% increase in cyberattacks, with one out of every 61 organisations globally affected by ransomware each week. By Q4, the upwards global trend continued, reaching an all-time peak by December, with 925 cyberattacks reported per entity each week.

According to the Check Point report, Africa experienced the highest volume of attacks in 2021, across five surveyed regions. Organisations in Africa had to deal with an average of 1,582 cyberattacks every week – a 13% increase from 2020. With a 75% increase in attacks compared to 2020, the education and research sector experienced the highest volume of cybercrime in 2021. Out of the 16 sectors surveyed, government and military came second, followed by communications, seeing a 47% and 51% increase respectively.

Insufficient funding

Considering the number of attacks seen just in 2021 and the disproportionate rise of cybercrime over just the last two years, institutions should take their intellectual property

security as seriously as is warranted and engage with methods to protect it as best they can. Intellectual property is extremely valuable to higher education organisations and adopting the correct technology to protect them is essential. In this regard, 85% of universities agree that more funding must be given to IT security to protect critical research IP (Purplesec, 2021).

Individual school establishments and cyberattacks

Emsisoft (2019) reported that at least 966 government agencies, healthcare providers, universities and colleges were compromised in a wide-scale ransomware attack that ended up costing over USD 7.5 billion. For example, a 2019 attack left 1,233 individual school establishments susceptible to attack. Because of the education industry's approach to cybersecurity and the end-users operating on campus, educational institutions are uniquely susceptible to attack.

Low cybersecurity rating of education institutions

Among 17 industries studied, the education sector ranked as the least secure, with the highest vulnerabilities being present in application security, endpoint security, and keeping software up to date regularly (EdTech, 2018).

Furthermore, in their 2020 Data Breach Investigations Report, Verizon (2020) found that educational establishments experienced the sixth-most amount of cybersecurity incidents out of 20 sectors, with 819 incidents. Data for 2022 suggests that the education sector has seen an increase in monthly cyberattack volume since 2021. For example, in the UK, government statistics indicate that 62% of higher education institutions reported experiencing breaches or attacks at least weekly in the previous 12 months (Sentinel One, 2022).

Device standardization which is so common in business is much harder to achieve in an educational setting. Also, awareness training should be encouraged so that end users are prepared when they are targeted by Social Engineering and similar attacks.

The list of cybersecurity incidents in higher education is going on but the above is sufficient to conclude that enhancing cybersecurity in the higher learning institutions in South Africa, including TVET colleges, is imperative.

CHAPTER 3: CYBERSECURITY CULTURE

CYBERSECURITY CULTURE OVERVIEW

Generally, cybersecurity culture is a subculture of an organisation's culture, which is often seen through the lenses of Quinn's "competing values" model, which distinguishes between four types of organisational cultures, based on the orientation of the values and beliefs (Quinn, 1988):

- The **support orientation** emphasises employees' spirit of sharing, cooperation, trust, individual growth, and the decisions made through informal contacts.
- The **innovation orientation** emphasizes that the organization is open to change, willing to search for new information, and willing to be creative in problem-solving.
- The **rules orientation** emphasizes respect for authority, formal procedures, and the importance of following written rules, normally resulting in a top-down hierarchical structure.
- The **goal orientation** emphasizes the specification of targets, the criteria for performance measurement and the reward based on the attainment of goals, reflecting the understanding of organizational goals, and individual responsibility and accountability.

Since organisational culture is tightly linked to people, it is not to expect that cybersecurity culture is different. Organisations of all types are vulnerable to cyber-attacks partially because people in the organisation are unaware of or unprepared for cyber risks. Building a culture of cybersecurity where the values, attitudes, and beliefs align with the organisational goals of cyber resilience is of significant interest to managers and leaders in charge of cybersecurity in organisations (Huang & Pearlson, 2019).

It is, unfortunately, happening that many times organisations overlook the human factor that cybersecurity depends upon. Hence, technology is often falsely perceived as the immediate answer to cybersecurity problems. However, cybersecurity is primarily a human factors problem, which remains unaddressed (Metalidou et al., 2014; Nobles, 2022). Humans do themselves pose a threat and vulnerability to the protection of information (Ismail & Yusof, 2018), hence, individuals must also take responsibility for maintaining a secure and vigilant culture at work, therefore, there is a need to develop and maintain a cybersecurity culture (Reegård et al, 2019).

Cybersecurity culture (CSC) is defined as the beliefs, assumptions, attitudes, values, perceptions, and knowledge that people have about cybersecurity and how these manifest in their interaction with ICT. A strong cyber security culture changes the mindsets of people and their security behaviour (ENISA, 2018).

Cybersecurity culture is also defined as the ideas, customs, and social behaviour of a particular people or society, i.e. behaviour of employees in an organisation that allows them to be free from danger or threats (Roer, 2013). However, the shortest definition of cybersecurity culture reads as "the way things are done here" (Brewerton & Millward, 2002).

It is accepted that cultivating a cybersecurity culture is an apt approach to promoting a secure consumption of cyberspace (Wamala, 2011). A cybersecurity culture aims to instil a certain way to 'naturally behave' in daily life, a way that subscribes to certain cybersecurity assumptions (Gcaza et al., 2015).

Due to the growing understanding that cybersecurity needs to be addressed also through organisational measures and not by technical measures alone, cybersecurity culture is attracting increasing attention. The results show that cybersecurity culture is understood as a sub-component of organisational culture comprised of more observable layers (Reegård et al., 2019). Technology alone cannot be a cushion against cyber threats, instead, humans should occupy centre stage through cybersecurity culture (Gcaza, et al, 2015).

Furthermore, Reegård et al (2019) believe that key practices for developing cybersecurity culture resemble those highlighted in the literature on safety culture: management support, policy, awareness and training, involvement, communication, and learning from experience.

Returning to the section dedicated to the needs of this study, da Vega (2016) suggests that individual cybersecurity culture can affect organisational, national, and international cybersecurity culture, and vice versa (Figure 3). This implies that raising cybersecurity culture within and through TVET colleges can influence the development of cybersecurity culture in the neighbouring communities – and, in that way, influence the national cybersecurity culture.

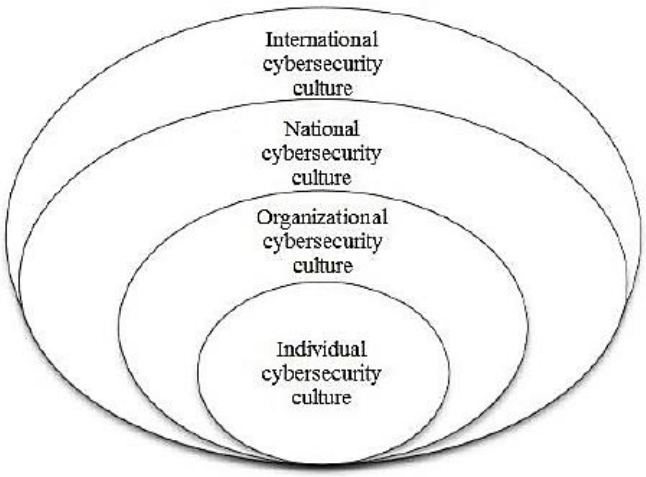

Figure 3 Cybersecurity culture levels (source: da Vega, 2016)

The development of the national cybersecurity culture will then contribute to the development of the international cybersecurity culture, which is outlined in the United

Nations 58/199 Resolution adopted by the General Assembly in 2004: “Creation of a global culture of cybersecurity and the protection of critical information infrastructures” (UNGA, 2004).

From a cybersecurity culture perspective, the organisational environment should be extended to a national and even international context, including the global connectivity of the Internet (da Vega, 2016). This, however, can only happen if first the community cybersecurity culture is developed. Da Vega (2016) added that how people utilise cyberspace can introduce risk to themselves, other individuals, organisations or even the country. Therefore, the attitudes, assumptions, beliefs, values, and knowledge of cyber users must promote efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, quality, and civil liberties when using cyberspace (NIST, 2014).

It is also worth noting that, although cybersecurity culture is attracting increasing attention, it is still a relatively new concept (Reegård et al., 2019). Only at the start of this century, did researchers begin to recognise that an organisation’s security culture might be an important factor in maintaining an adequate level of information systems security (Ruighaver et al., 2007).

It is important to understand that there are differences between cybersecurity culture and the more established concept of information security culture. The former lacks widely accepted definitions or guidelines and lacks widely accepted key concepts that delimit the culture (Reid & Van Niekerk, 2014; Gzaca and von Solms, 2017). It is believed that it is partly due to the concept being subject to different researchers’ perspectives and contexts of applications. As such, there is relatively little written about this phenomenon. In that regard, this study tests different perspectives of cybersecurity culture in the settings of TVET colleges in South Africa.

YOUTH AND THE SECURE USE OF ICT THROUGH DEVELOPING A CYBERSECURITY CULTURE

Most of the urban and rural youth live in the poorest countries but every year 14 million young Africans enter productive age and the majority live in remote areas. Globalisation and digitalisation mean that youth will have to find new paths for growth, opportunity, and employment than their parents.

At the same time, the overflow of information that comes with the digital boom often means that young people aspire to outpace the opportunities in their countries. Among the main factors hindering youth from self-sufficiency and independence is a lack of skills and individual capacity to drive change. It is, therefore, crucial to identify, understand and tackle these obstacles. In this regard, inclusive equitable policy and action are essential (SIANI, 2019).

Over the past few decades, the internet has evolved tremendously, which is evident from the fact that today, many people use the Internet for business, education, banking, and social

purposes. Although modern ICT provides some convenience and benefits, they also possess an opposite side in the form of cybersecurity threats. It is, thus, crucial that cybersecurity initiatives are undertaken to educate digital users. This is particularly important to those young technology users living in underdeveloped and rural and peri-urban areas where TVET colleges usually serve communities. On the other hand, it is important to educate youth regarding not committing cybercrime as there are serious low consequences, particularly related to the Cyber Crimes Bill, signed into law by President Cyril Ramaphosa on 1 June 2021.

There are a large number of works that show the usefulness of cybersecurity awareness and skills training as well as developing cybersecurity culture (Ernst & Young, 2017; Shouhuai, 2018; Huda, 2019; Beveridge, 2020). However, the literature review did not show readily available works on cybersecurity awareness, skills and culture related to the students, teachers, and managers of TVET colleges in South Africa. The importance of cybersecurity culture in TVET colleges is supported by the International Labour Organisation, which suggests that awareness of cybersecurity and data protection are skills required by TVET colleges (ILO, 2020). The study of Albrechtsen & Hovden (2010) also concluded that cyber awareness and cybersecurity culture play an important role in the online experience of individuals and needs to be addressed accordingly.

Minding the lack of relevant studies, we have conducted a genuine South African study, which aimed to produce a Conceptual implementation model for developing cybersecurity culture in TVET colleges and provide the guidelines for an Action plan for the development of cybersecurity culture in TVET colleges in South Africa.

STRATEGY ELEMENTS OF A SUCCESSFUL CSC PROGRAMME

Rumelt (2011) argues that a strategy that fails to define a variety of plausible and feasible immediate actions is missing a critical component. He argues that a strategy that fails to address which rational actions ought to be taken to meet the objective is mere 'fluff'.

The study by Gcza & van Solms (2017) proposes a strategy model for the national cybersecurity culture consisting of several elements (Goldman & Nieuwenhuizen, 2006; Enz, 2009; Tesone, 2012); Christiansen, 2014) as shown in Figure 4. As Gcza & van Solms's (2017) model is built upon some generic strategy elements, it justifies its appearance in this study. In other words, it is worthy of considering these elements for the development of the cybersecurity culture through TVET colleges. Each of these steps in Figure 4 is described by Gcza & van Solms (2017) in the following way:

Strategy direction

The strategic direction can be derived from the long-term objectives of the organisation. Some of them make use of statements that comprise the mission, vision, and values. Long-term objectives are always applied without fail.

Environmental assessment

The environmental-assessment process consists of the gathering and analysing of information, and then using the analysed intelligence in strategic decision-making. When conducting an environmental assessment, information can be gathered from different sources: personal and impersonal (also known as written sources).

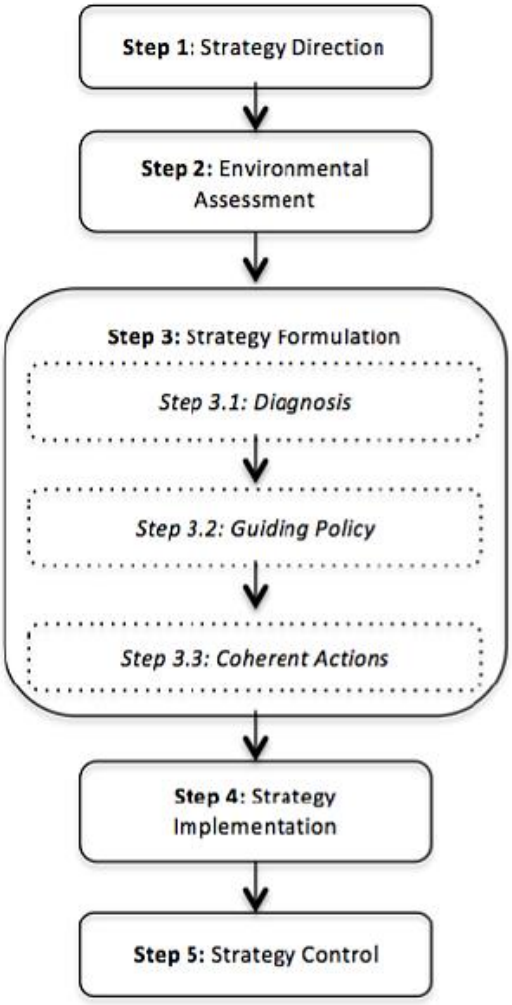

Figure 4: Cybersecurity culture strategy development model (source: Gcza & van Solms, 2017)

Personal sources include face-to-face communication, telephone communication, and various digitally-based communications, while written sources include various documents, reports, news articles and magazines. There are different modes of information viewing and searching (Aguilar, 1967):

1. **Undirected viewing**: This is viewing information without being led by a specific purpose.
2. **Conditioned viewing**: This is viewing information on selected areas guided by a specific purpose.
3. **Informal search**: This is a planned effort to obtain information on a specific issue.

4. **Formal search**: This is an unstructured effort of actively looking for information.

Strategy formulation

The strategy formulation process consists of three sub-processes:

- **Diagnosis** stems from environmental assessment.
- **Guiding policies**, which suggests that the guiding policies and coherent actions are extrapolated from the existing cybersecurity implementations (e.g. Global Cybersecurity Index, Cyber wellness ITU Report, etc).
- **Coherent actions**: This should be guided by the set of diagnoses to ensure the applicability and suitability of the recommendations.

Strategy implementation

Most strategies fail to be implemented due to the challenges and complexities of strategy implementation (Rumelt, 2011). Hence, before the process of implementing strategy, it is important to ask the following questions (Wheelen & Hunger, 2012):

1. Who are the people who will implement the strategy?
2. What needs to be done to implement the strategy?
3. How is everyone going to work together to do what is needed?

The first question focuses on identifying the people needed to implement the strategy. The second question implies drafting programs, budgets, and various procedures. The third question deals with possible restructuring in the organisation in such a manner that would be conducive to executing a new strategy. This involves ensuring that each program is staffed with adequate personnel.

Strategy control

Strategy control is intended to ensure that the stipulated strategic objectives are achieved through five steps (Goldman & Nieuwenhuizen, 2006; Enz, 2009; Wheelen & Hunger, 2012):

1. Determine what to measure.
2. Establish standards of performance.
3. Measure the actual performance.
4. Compare the actual performance with the established standard; and
5. Take corrective action, if necessary.

The above steps require that all the implementation processes will be measured. Subsequently, the performance measures must be defined. Such measures should be then compared with the actual performance of the implementation processes. If necessary, corrective actions should be taken.

DIMENSIONS OF CYBERSECURITY CULTURE

In cybersecurity, there are three interrelated pillars that organisations need to build and maintain: people, tools, and processes. The people aspect, and in particular the understanding of how people use tools and processes, is little understood (Laycock et al., 2019).

The Laycock et al., 2019 cybersecurity culture model includes this little-understood component and is an important element of a wider Security Culture Framework. The model consists of seven dimensions: attitudes, behaviour, cognition, communication, compliance, norms, and responsibilities.

ATTITUDES

This relates to feelings and beliefs that employees have toward cybersecurity protocols and issues. Attitudes are commonly expressed in terms such as prefer, like, dislike, hate, and love. Attitudes involve a preference for or against something. The Theory of Planned Behaviour (later progressed into the Theory of Reasoned Action) exposes attitudes as an important antecedent of behavioural intent (Ajzen & Fishbein, 2005).

When we express our attitudes, we are expressing the relationship (either positive or negative) between the self and an attitude object. Attitude objects can be a person, place, thing, or idea. These objects are those things that a person makes a judgment about or has a feeling toward. These judgments or feelings about the attitude objects can be either positive or negative (Jhangiani et al., 2014; Laycock et al., 2019). For example:

"*I like my security badge*," "*I hate changing my password*," or "*I love my job*."

Social psychology has discovered that our attitudes are made up of cognitive, affective, and behavioural components. Jhangiani et al (2014) provide the following illustrative examples considering an environmentalist's attitude toward recycling, which is probably very positive.

In terms of **effect**: They feel happy when they recycle.

In terms of **behaviour**: They regularly recycle their bottles and cans.

In terms of **cognition**: They believe recycling is the responsible thing to do.

This has significance for cybersecurity research as quite often participants may not have activated attitudes towards cybersecurity or the protection of information (Laycock et al., 2019). Exploring people's attitudes towards cybersecurity provides an important metric to help target awareness more proactively. Negative attitudes, for example, are manifested by people who see reporting cyber incidents as a waste of time (Hadlington, 2018). Hence, measuring the attitudes of people toward cybersecurity policy is essential for an organisation to get an estimate of overall sentiment toward cybersecurity issues in an organisation (Laycock et al., 2019).

BEHAVIOUR

The behaviour relates to the actions and activities of people that have a direct or indirect impact on the security of the organisation. The behaviour of people, the most researched topic in the ICT field, is a direct cause of cybersecurity breaches and incidents as employees can execute activities of great threat to organisational assets (Herath & Rao, 2009; Crossler et al., 2013; Safa et al, 2015). Whether they act intentionally or unintentionally, in our industry, these employees are referred to as insider threats or insiders (Laycock et al., 2019).

For example, there are different types of users and many of them behave in a non-malicious way. However, these users have low technical knowledge related to, for instance, password creation and sharing. It is often found in various reports that most users reuse the same password from site to site, and most of them rely on the same patterns when making passwords (Stanton et al, 2005; Sandler, 2018).

Another unintentional but potentially harmful behaviour is carelessly clicking on phishing links in emails and on websites. Visiting non-work-related websites using the company's computers, and unintentionally posting confidential data onto unsecured servers or websites are also potentially dangerous behaviours.

Opposite of these non-intentional actions are so-called "deviant behaviours". This type of behaviour describes those actions which are intentional and are often labelled as sabotage, stealing, and industrial or political espionage (Crossler et al, 2013).

Behaviours are generally very difficult to change, but Laycock et al. (2019) suggest that it is possible. The most popular social psychology work among cybersecurity researchers seems to be the Theory of Planned Behaviour. This theory sees behaviour as a function of a person's attitude toward the behaviour, the norms that people around the person have (e.g. social pressure), and the person's feeling of control over their behaviour (e.g. how easy it is for the person to perform one behaviour (Safa et al., 2015).

The organizational culture that develops based on exhibited behaviour is evident in artefacts (e.g. using encryption), values (e.g. "the privacy of customer data is respected"), and basic assumptions (e.g. "executive management understands the information risk") (Schlienger &Teufel, 2005; da Vega, 2016).

COGNITION

Cognition corresponds to the people's understanding, knowledge and awareness of security issues and activities. It is argued by Laycock et al. (2019) that if a person is not aware of basic concepts of cybersecurity, he or she is more prone to cybersecurity threats than others. Hence, knowledge is one of the key concepts in the research of human factors in information security, and it is a dominant component of cybersecurity awareness (Herath & Rao, 2009).

ENISA's (2010) report also asserts the importance of knowledge for cybersecurity culture, through awareness training and changing behaviour. In general, a cybersecurity awareness programme is expected to:

- **Communicate cybersecurity knowledge** (i.e., recommended guidelines and security best practices) to the target audience.
- **Broaden** the **cybersecurity knowledge** of the target audience (i.e., familiarity with guidelines and security best practices), hence,
- **Bring positive changes** in **attitude** (i.e., motivate to adopt recommended guidelines and practices) and behaviour (i.e., create a strong culture of security) in the target audience.

However, the relation between knowledge and behaviour is not direct and linear (Kaur & Mustafa (2013) but the knowledge gained by employees can provide reliable insight into which processes are important to monitor and improve to strive for a change in employee behaviour (Roer & Petric, 2017).

The notion of cognition typically refers to a range of mental processes relating to the acquisition, storage, manipulation, and retrieval of knowledge. Farooq et al (2015) believe that there are three cognitive skills necessary for an effective learning experience: (1) knowledge of facts, processes, and concepts, (2) ability to apply the knowledge, and (3) ability to reason. These cognitive skills are developed through thought, experiences, and senses.

Measuring the organisation's cognition of cybersecurity indicates what employees verifiably know or believe, what they understand of security-related issues and practices, as well as how they apply their knowledge (Laycock et al, 2019).

COMMUNICATION

This relates to the quality of communication channels for discussing security-related events, promoting a sense of belonging, and providing support for cybersecurity issues and incident reporting. Communication is a mechanism for securing or compromising information through the management of people and technology (Backhouse & Dhillon, 1996). Communication also plays a vital role in organisational cybersecurity (Arhin & Wiredu, 2018).

The significance of communication is also reflected in the IBM Cost of Breach report 2018 stating that it takes an average of 197 days for organisations to detect a breach and a further 69 days to resolve the situation and restore service (IBM, 2018).

While communication is a basic requirement of management, it is also instrumental in raising the morale of employees, affecting motivation, and encouraging employee engagement (Laycock et al, 2019). The same authors also state that empirical research on the role of communication in cybersecurity culture is rare but important as it shows that both the prevention of security breaches and the response to them are largely determined by effective

communicative processes. This study on the cybersecurity culture at TVET colleges will, hence, add to the still scarce body of literature on the topic of the role of communication in cybersecurity.

COMPLIANCE

Data breaches are related to larger issues, including compliance (Chatterjee & Sokol, 2019). This and similar findings suggest that cybersecurity compliance is a well-researched topic. The reviewed literature suggests that non-compliance to cybersecurity standards and policies is one of the main human-related reasons for cybersecurity breaches in organisations (Al-Kalbani et al., 2014).

Compliance refers to knowledge of written cybersecurity policies and the extent that people follow them. Cybersecurity compliance ensures that security mechanisms implemented in an organisation work together effectively to protect critical information (Kim et al., 2016).

Compliance includes many organisational processes, hence, enforcing security compliance is a complex cybersecurity culture issue (Safa et al., 2016). According to Al-Kalbani et al., (2017), the adoption of cybersecurity compliance in organisations involves:

- **Implementation** of effective and balanced cybersecurity measures and mechanisms.
- **Compliance** with legal and security requirements and expectations of organisations.
- **Maintaining** both employees' and stakeholders' confidence and trust in the security.

Having a well-documented set of policies and procedures is not, by itself, good enough to deter cybersecurity breaches (Safa et al., 2016). The most used approach nowadays is that of the already mentioned Theory of Planned Behaviour.

In addition to having a well-documented set of policies and procedures, cybersecurity policies must be clearly understood, readily available and easily accessible to all employees. Compliance can be improved when the employee understands how the policy affects them, their work activities, and their role within the organisation (Laycock et al, 2019).

NORMS

Norms are typically understood to be one of the most important mechanisms that influence humans**,** thus a key element of a cybersecurity culture. Sociological, socio-psychological and behavioural cybersecurity researchers suggest that norms guide employees in their use of organisational information systems and highlight norms as one of the key elements that characterise end-user security behaviour and compliance (Hechter & Opp, 2001; Siponenet al, 2010; Laycock et al, 2019).

Laycock et al (2019) suggest that a socio-psychological Theory of Planned Behaviour is generally adopted by the cybersecurity field. This theory shows that people generally orient their activities based on reasoning, i.e. "if other people who are important to me think I should

do X, then it is probably smart to do X". However, Bicchieri (2016) warns that, although norms are very powerful, they are difficult to influence as they are a relatively stable set of unwritten rules regarding what is good, right, and important. Hence, the task of a building cybersecurity culture is to stimulate the development of norms that support organisational cybersecurity and ensure these norms become internalised (Laycock et al, 2019).

Also, personal norms can be influenced by external sources. For example, these are social norms or factors such as awareness of consequences and ascription of personal responsibility (Gavrilets & Richerson, 2017). Therefore, Laycock et al (2019) suggest that, instead of directly appealing to people's moral obligation, an organisation may, via social norms, persuade its employees to behave accordingly.

RESPONSIBILITIES

The notion of responsibilities relates to how people perceive their role as a critical factor in sustaining or endangering the security of the organisation. In other words, responsibility is mainly related to employees' practices and performance such as monitoring and control, reward and deterrence, and acceptance of responsibility (Al-Hogail, 2017).

Employees must be aware that knowing and practising secure behaviour is their responsibility and that the protection of information and information systems should be part of their daily activities (Thomson et al, 2006). Organisations cannot truly protect their assets without ensuring that employees understand their roles and responsibilities and that they are sufficiently trained to perform them (Furnell & Thomson, 2009).

However, Laycock et al (2019) caution that, although employees can know about cybersecurity issues, have positive attitudes and have a generally good awareness of security issues, they need to be fully aware of their responsibilities and roles in securing their organisation. In this way, employees will proactively engage in resisting and reporting cybersecurity incidents.

Laycock et al (2019) add that responsibilities can be influenced by clearly defining the roles of employees regarding cybersecurity. If the members of an organisation do not understand their place in the security of the organisation, they are less likely to follow the necessary steps and procedures to make the organisation safe.

Note on the research in the field

A lot of research on the topic is hindered by the fact that it only collects data from IT administrators or top-level managers and there is hardly any representation from the end-user community (Herath & Rao, 2009). Hence, apart from managers, this study includes end-user (TVET colleges' students and teachers) behaviour (Laycock et al., 2019).

LAYERS OF CYBERSECURITY CULTURE

Organisational culture is, by some authors, viewed as manifested in three levels: tacit assumptions that are beliefs about reality and human nature; espoused values that refer to social principles, philosophies, goals, and standards; and artefacts that are visible, tangible, and audible results of activity grounded in values and assumptions (Hatch, 1993).

This concept of organisational culture has been the basis for most models or frameworks of cybersecurity culture (Connolly & Lang, 2012). However, Reegård et al (2019) argue that, in cybersecurity, some authors add, the fourth layer of knowledge. It is believed that knowledge will influence assumptions, values, and behaviours (ENISA, 2018; Van Niekerk & von Solms, 2010).

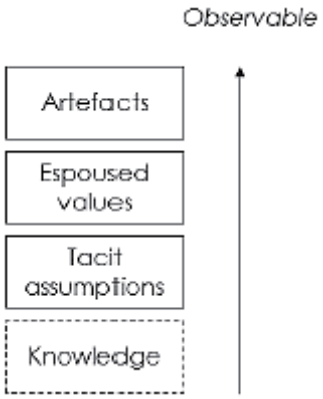

Figure 5: Illustration of the layers in cybersecurity culture (source: Reegård et al, 2019)

The layers of cybersecurity culture are interconnected and understanding each may be necessary for ensuring the implementation of adequate measures (Van Niekerk & von Solms 2010). For example, understanding the values that drive people's actions can contribute to a greater understanding of compliance issues with cybersecurity policies (Hedström et al, 2011). However, values and assumptions are often the more difficult layers to address as these must be inferred from what members of the organisation say and do. Consequently, most literature on cybersecurity culture addresses the observable layer of artefacts and behaviours (Reegård et al., 2019).

Reegård et al (2019) also note that there is little specific mention of the content of such a fourth layer in the literature on cybersecurity culture in general, or it is indirectly addressed through the three other layers. Hence, they promote the three-layer cybersecurity culture model (Figure 6).

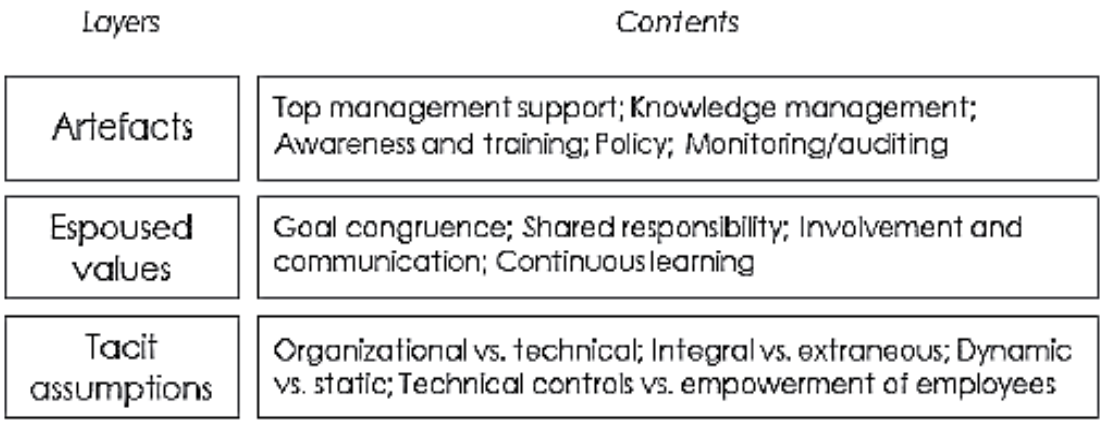

Figure 6: The concept of organizational cybersecurity culture consisting of layers adhering to Schein's model (source: Reegård et al, 2019)

TACIT ASSUMPTIONS

Tacit assumptions are beliefs about reality and human nature (Hatch, 1993). Viewing cybersecurity as an integral part of conducting business is important for avoiding contradictory narratives in the organisation that can reduce the effectiveness of cybersecurity roles and measures. For example, an organisation that views cybersecurity as integral to business is likely to strive for a balance between cybersecurity goals and goals of other business areas. An assumption whether cybersecurity is primarily an organisational issue or a technical issue is a tacit issue. (Reegård et al, 2019). View of cybersecurity as something static versus dynamic is also an example of tacit assumptions (Ruighaver et al., 2007).

ESPOUSED VALUES

The assumptions matter as these are linked to the embraced values and the rationale of the organisation in how to best manage cybersecurity and cybersecurity culture (Barton et al, 2016; Al-Izki & Weir, 2016). Whether cybersecurity is seen as a responsibility of the whole organisation or specific parts of it also represents value. An example is the issues when technical personnel may have if they are left to manage cybersecurity in isolation. For instance, if Chief Information Security Officers (CISO) struggle between contradictory pulls in the organisation that rendered their role and efforts in cybersecurity less effective by needing to seek constant buy-in from employees (Ashenden & Sasse, 2013).

ARTEFACTS

The beliefs and values of the organization about cybersecurity translate into observable behaviours and practices or non-practices (Reegård et al, 2019). The top management's active participation, championing and/or financing of cybersecurity activities are, for example, the most mentioned in the pertinent literature. Cybersecurity awareness and training programs and cybersecurity policies are also well-known artefacts of cybersecurity culture (e.g. Ashenden & Weir, 2016; Steinbart et al, 2018).

CYBERSECURITY CULTURE PRACTICES

Reviewing the apposite literature, Reegård et al (2019) found out that the works on cybersecurity culture often aim to identify how organisations can develop that type of culture. These are the main practices that they discovered:

Management support

Management support can come in a variety of forms. It ranges from a willingness to financially invest in initiatives and advocate for cybersecurity, to the organisation of the cybersecurity function and follow-up on cybersecurity work and status. This kind of support is vital for creating and maintaining a focus on cybersecurity and heavily influential on the performance of other cybersecurity practices. For example, active participation and visible support by top management are of major importance to the formulation and implementation of cybersecurity policies (Karyada et al, 2005).

Cybersecurity policy

As that cybersecurity culture is a management issue, one of the key practices is to establish an internal policy to demonstrate management intent and the importance of cybersecurity. When people are aware of the organisational cybersecurity policy, they can better manage cybersecurity issues (Li et al., 2019). Cybersecurity policies also provide overall guidance in building a cybersecurity culture (Knapp et al. 2009). In devising cybersecurity policies, it is important to find a balance between management and employee perspectives to make such policies useful.

Cybersecurity policy is an artefact that results from a dynamic process and that should itself be dynamic, i.e. frequently updated following the information provided from other activities and changing risks (Knapp et al, 2009). Karyada et al. (2005) also believe that the application of cybersecurity policies is dynamic and that it is necessary to understand the contextual factors that may affect its adoption.

Minding the above, the employee perspective is part of the contextual factors that may influence policy adoption and should be addressed through the policy process (Reegård et al, 2019). In general, cybersecurity documentation provides all necessary documentation and allows people to recognise cybersecurity awareness concerns and respond accordingly (ENISA, 2010). The policy document aims to enhance the knowledge and cybersecurity awareness of learners in South Africa (Walaza & Kritzinger, 2019).

Cybersecurity awareness and training

Metalidou et al. (2014) identified five factors that can seriously impact how people behave concerning cybersecurity:

- **Lack** of **motivation.**
- **Lack** of **awareness**.

- **Inaccurate beliefs** about behaviours or risks.
- **Risky behaviour** and inadequate use of technology.

Minding these factors and the fact that knowledge, both of management and employees, is one of the cornerstones in shaping cybersecurity culture, Metalidou et al. (2014) concluded that cybersecurity awareness is the key to mitigating security threats caused by human weaknesses.

Agreeing that awareness is an important factor in cybersecurity culture, ENISA (2010) report states that, in general, a cybersecurity awareness programme is expected to:

- Bring **positive changes** in attitude (i.e., motivate to adopt recommended guidelines and practices) and behaviour (i.e., create a strong culture of security) in the target audience.
- Gain and **keep** the audience and management or sponsor **trust** and **satisfaction**, and ultimately,
- **Minimise** the number and extent of security **breaches**.

To increase awareness of cybersecurity, the organisation must ensure that the training is tailored to the target population as people interpret and internalise risk-related information through the lenses of cognitive and cultural bias (Thsohou et al, 2015). Hence, Van Niekerk & Von Solms (2010) believe that it cannot be assumed that the average employee has the necessary knowledge to perform his/her job in a secure manner. Thus, cybersecurity awareness training is one of the cornerstones of a cybersecurity culture. In this regard, It is important that cybersecurity training is interesting and engaging. Conversely, Cone et al. (2007) argue that many forms of training fail because they are repeatable and do not require users to think about and apply security concepts.

Involvement and communication

Employees can identify cybersecurity issues as they emerge and creatively address them based on their work experiences and knowledge, argues Lin and Wittmer (2017). Their study showed that employees have the potential to positively contribute to cybersecurity if their participation is encouraged which, in turn, promotes proactivity.

One of the best ways to improve motivation is through broad horizontal participation, i.e. peer-to-peer participation (Ruighaver et al, 2007). This will require genuine two-way communication between the management and employees, negotiation, and involvement to overcome the often observed ‘them’ and ‘us’ relationship (Ashenden & Sasse, 2013). This is supported by Flores et al. (2014) who believe that cybersecurity knowledge sharing can contribute to mitigating risks. The underlying coordinating processes related to risk management and performance monitoring are essential for the establishment of knowledge-sharing mechanisms.

Learning from experience

Monitoring of specific outcomes is used to validate or falsify current beliefs regarding the organisation's cybersecurity (Kearney & Kruger, 2016). Auditing is another example of such a mechanism that can help in increasing the organisation's awareness of its internal cybersecurity environment (Reegård et al, 2019). On the other hand, organisations may fall into a trap of an external focus when having an external audit in which the organisation is primarily focused on succeeding in the audit rather than achieving the security they need (Ruighaver et al, 2007).

The use of maturity models is another example of how some organisations attempt to establish their current level of cybersecurity and identify further focus areas for improvement. An important mechanism that enables learning is incident reporting systems whose primary purpose is to share information on incidents to avoid their reoccurrence or limit the damage they can cause (Reegård et al, 2019).

IMPLEMENTATION OF CYBERSECURITY CULTURE STRATEGIC GUIDELINES

ENISA FRAMEWORK

The research literature did not show many appropriate works in cybersecurity strategies, but the ENISA cybersecurity culture framework appeared to be relevant to this study. It is centred on specific activities, their implementation and measurement of impact. The approach of this framework is iterative in that after each cybersecurity activity is run, the impact is measured, results considered, and the approach is reviewed. Following this, new activities may be chosen, or delivery methods may be changed. This also allows for considering and amending initial goals and/or the target audience (ENISA, 2018).

The ENISAs cybersecurity culture strategic guidelines are given in the following steps (Figure 7):

Step 1: Set up the core cybersecurity culture workgroup

This group will be tasked with knowledge generation to ensure an evidence-based approach to cybersecurity as well as the formation of the cybersecurity culture programme and strategy, overseeing the implementation of the relevant activities, and ensuring alignment with the organisation's cybersecurity policies. Bringing together a core team from specific areas within an organisation maximises the potential for the future success of that organisation's cybersecurity culture programme. This core team also requires the support of senior management to champion this programme.

Step 2: Business understanding and risk assessment

This step involves understanding what values, cultures, beliefs, and practices already exist within the organisation and why they are there. This knowledge is likely available within each

department and team. It is important to look at the different needs of each team/department and specific job roles as these may differ quite substantially and there might be barriers to success that will be uncovered unless consulted with employees. An essential element in this process of understanding the business is mapping and assessing the current/future cybersecurity measures implemented by the security team against the processes that must be undertaken within each business unit if those employees are to fulfil the requirements of their roles.

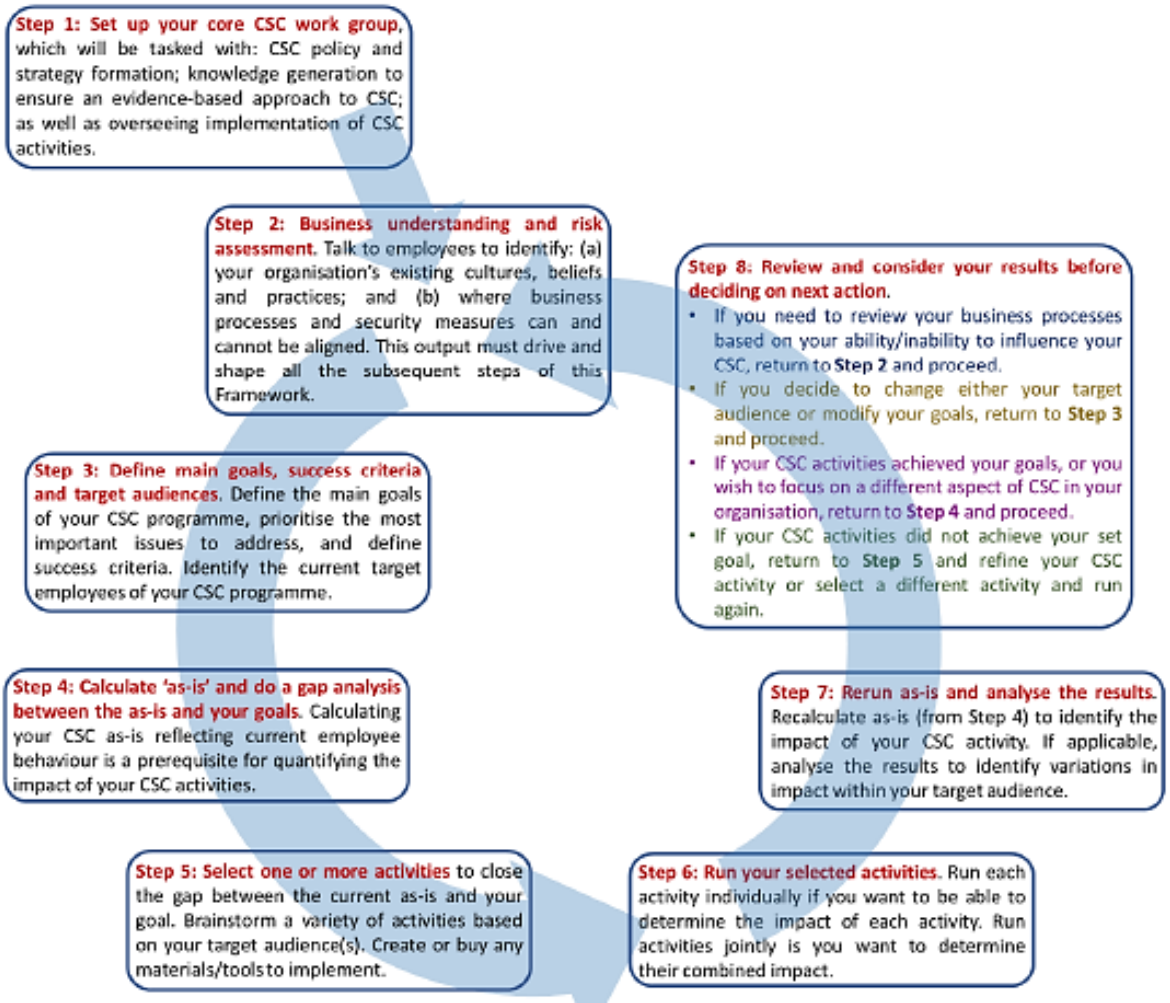

Figure 7: Step-by-step framework for organisations to implement a CSC programme (source: ENISA, 2018)

Step 3: Define main goals, success criteria and target audiences

For each organisation, it is important to clearly define the main goals, and the associated success criteria for judging when these goals are met, about the organisation's future cybersecurity culture. When doing so, it should be recognised that some of these goals will have universal application across the entire organisation, while others will be targeted at specific groups and roles. This process of defining goals and the associated success criteria

will assist with calculating the current cybersecurity culture situation and defining metrics in Step 4.

Step 4: Calculating the current situation and do a gap analysis between the current situation and the goals

It is not possible to quantify the impact of future cybersecurity culture programmes if the current situation is not established. In assessing the current situation, it is important to do a gap analysis between the current situation and the goals. There are three main approaches to doing that:

1) Determine the cybersecurity culture's current situation independently from the proposed interventions.
2) Determine the cybersecurity culture's current situation by utilising the intervention metrics.
3) Combine approaches 1 and 2.

Step 5: Select one or more activities

The chosen activities must be linked to the current situation and goals, and it is needed to determine the right tactics to adopt when selecting and deploying the activities. To this end, some questions need to be considered: (1) What topics are focussing on, (2) What is the messaging when addressing these topics, and (3) What is targeted (i.e., people, processes, or technologies)? It is also needed to select the medians/activities that are going to be used - for example, changes to policies/processes, software changes, awareness-raising programmes (posters, email campaigns, etc.), training sessions, scenarios, and wargames, using incentives, etc.

Step 6: Run your selected activity

The selected activities should be run individually if they want to be able to determine the specific impact of that activity. The activities should be run together as a joint set if the intention is to determine the combined impact of those activities. These activities should be monitored closely while they are being run to ensure they are being conducted correctly. In that regard, the best method should be selected for achieving the results based on the context of both the activity being run and the organisation’s resources.

Step 7: Rerun the current situation metric and analyse the results

After the activity (or joint set of activities) is completed, it is needed to rerun the cybersecurity culture measurement compared to the current situation and goals (Step 4) and analysed the results to identify impact (i.e., levels of success and any failures). These results can also be used to identify whether any positive or negative effects were universal across the entire target audience, or whether they varied by different sub-sets of the audience: e.g. specific age groups, business units, countries, roles, etc.

Step 8: Review and consider your results before deciding on the next action

This step is the chance to review the strategy, based on the findings and experiences, and determine how the cybersecurity culture proceeds going forward. If the cybersecurity culture activities did not achieve the set goals, return to Step 5 and refine the activities or select a different [set of] activities and run again. If the cybersecurity culture activities achieved the goals, or if an organisation wishes to focus on a different aspect of cybersecurity culture, return to Step 4 and proceed. If the target audience should be changed or the goals modified, return to Step 3 and proceed. If based on the ability or inability to influence the organisation's cybersecurity culture, it is needed to reassess the business processes and/or cybersecurity measures, return to Step 2, and proceed.

THE CURRICULUM OF THE EDUCATIONAL COURSE ON CYBERSECURITY CULTURE

Inclusion of threats in cybersecurity education

A general approach to the cybersecurity curriculum should include topics on different cyber threats. In that regard, Whitman and Mattord (2017) suggest the 12 categories of threats (Table 1):

Table 1: Twelve categories of threats to information security (source: Whitman & Mattord, 2017)

Category of threat	Attack example
Compromises to intellectual property	Privacy, copyright, infringement
Deviations in quality of services	Internet service provider (ISP), power, or WAN service problem
Espionage or trespass	Unauthorised access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning
Human error failure	Accidents, employees' mistakes
Information extortion	Blackmail, information disclosure
Sabotage or vandalism	Destructions of systems or information
Software attacks	Viruses, worms, macros, denial of services (DoS)
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

Cybersecurity awareness, training, and education

Whitman and Mattord (2017) suggest the following framework for cybersecurity awareness, training and education framework (Table 2):

Table 2: Framework of security awareness, training and education (source: Whitman & Mattord, 2017)

	Awareness	Training	Education
Attribute			
Level			
Objectives			
Teaching method			
Assessment			
Impact timeframe			

Cybersecurity culture-related education

The motivation for the Cybersecurity culture course inclusion in the curriculum is based on making employees (particularly IT professionals) capable of formulating and arguing their proposals, to convince the organisation's top management of the need to take measures to protect information and to be able to work with the staff (Malyuk & Milosavskaya, 2016).

However, there is still no official curriculum focusing on cybersecurity in South African schools. It is typically left to higher education to educate students on the principles of cybersecurity, predominantly related to computer-related modules (Venter et al., 2019).

The main topics for the curriculum related to cybersecurity culture, as proposed by Malyuk & Milosavskaya (2016) include:

- The strategy of information society development.
- Information culture and ethics.
- Information support of public policies.
- Information and psychological security, psycho-physical effects on the individual and society, and information weapons.
- The Internet and freedom of speech; protection from malicious content.
- Social challenges of the information society; the problems of education and training.
- Legal issues of information society development; protection of intellectual property.
- The IT crime.

The content of the same course taught in another educational institution may differ significantly from the proposed one. It depends on many factors, such as the curriculum focus, the duration of the course, the term on which the course is taught, the local specifics of the country and region where the university is located and so on.

ORGANISATIONAL FACTORS IMPACTING CYBERSECURITY CULTURES

Organisations can take steps to shape both their cybersecurity culture and wider organisational culture can greatly influence cybersecurity culture. Here, collaborations within the organisation are essential as open communication will facilitate the development of a

cybersecurity culture. While everyone within an organisation should be involved, contributing their fields of expertise, identifying where cybersecurity risks and other business functions intersect, and potentially conflict and brainstorming solutions, certain executive positions and departments have a key role to play in the development of the cybersecurity culture. These factors are examined below (ENISA, 2018).

ORGANISATIONAL CULTURE

Organisational culture is a complex system of shared beliefs and values among employees, which guides their behaviour or to put it simply, it is the way things are done. The people's cybersecurity views, attitudes and behaviours will in turn be affected by changes in the organisation's cybersecurity culture. Organisational culture can reinforce the commitment to the organisation and enhance stability by offering guidance and accepted standards for people's behaviour. Both acceptable and unacceptable behaviour should be defined in line with the organisation's intentions and encouraged or denounced respectively. If sanctions are enforced, consistency in their application is needed to ensure compliance and influence changes in the mindsets of people (Alnatheer et al., 2012).

Against this backdrop, an effective cybersecurity culture should be fully embedded within the organisational culture if the value of cybersecurity is to be accepted by all members. Indeed, a commitment to quality and cybersecurity suggests a wider organisational culture of excellence in organisations (RAND, 2008).

THE ORGANISATION'S WIDER CYBERSECURITY STRATEGY

A pre-requisite for a cybersecurity culture is the development and communication of policies and procedures, which lay down clear responsibilities and serve to guide security behaviour and attitudes. Based on an initial assessment of the current state of cybersecurity culture, management should draft a cybersecurity strategy incorporating a policy to guide the cultural change and define security goals and the organisation's vision. In so doing, specific goals and end-user usability should be fundamental considerations, as permanent behavioural changes are possible only when they equate to success and satisfaction among people.

A successful strategy should: (1) reinforce strong governance attitudes and actions; (2) be designed similarly to other business functions to ease acceptance; (3) be built around an adaptable framework to facilitate long use; and (4) its effectiveness should be measurable to demonstrate success (ENISA, 2018). The use of metrics here can aid management in reviewing and updating policy through regular monitoring and assessment of impact.

Strategy control is also important and is intended to ensure that the stipulated strategic objectives are achieved and comprises five steps (Wheelen & Hunger, 2012):

1. Determine what to measure.
2. Establish standards of performance.

3. Measure the actual performance.
4. Compare the actual performance with the established standard, and
5. Take corrective action, if necessary.

The above steps recommend that the appropriate body specify all the implementation processes that will be measured. The performance measures must be defined in the next step. Such measures should subsequently be compared with the actual performance of the implementation processes. Finally, corrective actions should be assessed and taken (Gcza & van Solms, 2017).

CROSS-ORGANISATIONAL COMMITMENT – THE ROLES TO BE PLAYED BY DIFFERENT GROUPS

The role of senior management

Cyber security has become the responsibility of senior management, driven by the financial and reputational risks of breaches, regulatory requirements and pressures exerted by shareholders. Beginning, transmitting, and embedding cultural change requires leadership and buy-in by senior management. It is also needed to ensure that this change is lasting so that it signals management's commitment and involvement in cybersecurity culture by allocating sufficient resources for comprehensive programmes while delegating clear responsibilities and authority (Alnatheer et al., 2012)

The role of CISOs

Chief Information Security Officers (CISOs) have a crucial role in developing a cybersecurity culture. She or he must understand the needs and operations of the business while using their technical and communication skills to align IT and cybersecurity goals with business ones. CISOs should then participate in drafting the cybersecurity strategy and represent cybersecurity at the executive level while maintaining good communication channels with both senior management and employees to effectively share their vision (Ashenden, 2008). To the management and the board, the CISO should make clear the value of cybersecurity, while offering information on cybersecurity developments, risks and options in line with risk management.

The role of middle management

As the intermediary between employees and senior management, middle management has a key role to play in setting the tone of cybersecurity in an organisation. They need to be convinced of its benefits and should be effectively involved in the implementation of cybersecurity throughout the organisation. To avoid cybersecurity being treated as an impediment and burden by the teams they lead middle management should insist on and encourage secure behaviour by offering feedback and motivation for employees, both regarding their business and IT performance.

The role of the IT department

The role of the IT department team in cybersecurity culture is multifaceted. The team should ensure that up-to-date technical measures are adopted, which are effective, simple, useful and support secure behaviour by not being overly burdensome. To effectively achieve these aims by tailoring solutions, those maintaining the technical infrastructure must understand the business structure of their organisation and its activities, while the open communication of IT objectives, milestones and processes can further guide the cybersecurity culture programme (RSA, 2017).

The role of legal/compliance

The legal and compliance department has a role to play by offering expert legal advice to ensure any cybersecurity culture and cybersecurity practices embedded in the organisation comply with national and international legislation, including data protection norms. The department should also provide support when implementing technical measures geared towards monitoring employee behaviour, to establish that what is being monitored and how the information is utilised is fully compliant with national and transnational legal requirements.

The role of Human Resources

Human resources (HR) have an important role as a connector between management and employees. Thanks to their position within an organisational, HR can offer insights into the behaviour and psyche of employees, which in turn can be used to counter potential insider threats or design and deliver effective security education programmes. The department can also ensure that everyone in the organisation undergoes the necessary security training by enforcing compliance while conducting security practice evaluations of employees and, where necessary, enacting disciplinary sanctions (ENISA, 2018).

The role of marketing and internal communications

Cybersecurity culture is about changing mindsets, and perceptions and conveying knowledge to people, with cybersecurity presented to employees as “business as usual”. The marketing department can assist in the development of a cybersecurity culture by designing and promoting cybersecurity awareness and education programmes, and producing messaging that maximises impact and emphasise the benefits of a cybersecurity culture. They can also maximise cost-effectiveness by leveraging personalised approaches and multiple channels (Bernik et al, 2008).

HUMAN FACTORS IN CYBERSECURITY CULTURE

Managing employees’ security behaviour is still a major challenge. Johnson & Goetz (2007) cite Theresa Jones, a security manager at Dow Chemical: “My biggest challenge is changing behaviour. If I could change the behaviour of our workforce, then I would think I had solved

the problem" (Beautement et al, 2008). In that regard, cultivating a cybersecurity culture is viewed as the best approach for addressing the human factors that weaken the cybersecurity chain since even users who possess more cybersecurity knowledge can behave similarly to those who lack any form of cybersecurity awareness (Van Niekerk & Von Solms, 2010).

Cybersecurity technologies can be effective only when people have the necessary knowledge, skills, understanding and acceptance to use those (Furnell & Thomson, 2009). However, reaching human security may require a change in both the knowledge and behaviour of people (van Niekerk & von Solms, 2005). Furthermore, education and training may be used to foster knowledge, while behaviour can be altered through cultural and organisational incentives and sanctions (van Niekerk & von Solms, 2005a).

The human factor is a big issue when it comes to cybersecurity awareness in developing countries like South Africa. Furthermore, factors such as low levels of education or inadequate education are major problems in many developing countries (Walaza & Kritzinger, 2019).

PSYCHOLOGICAL FACTORS

To convince people to change, three parallel processes must take place: (1) there must be dissatisfaction with the current situation, (2) this dissatisfaction must cause anxiety and/or guilt, and (3) employees must be able to adopt new behaviour in a safe environment without compromising their identity or integrity (Schein, 2004).

To 'unfreeze' the existing culture, its shortcomings must be identified and communicated, after which the new culture can be instilled by changing knowledge and behaviour. This must be conducted in a safe learning environment to prevent anxiety and defensive attitudes against the new culture. Coercion should be avoided, as it would increase defensiveness and decrease acceptance of the change (Schein, 2004; van Niekerk & von Solms, 2005). Instead, people must be engaged in the culture so that they participate in, contribute to it, and feel responsible for it. This can be achieved through accountability, trust, communication, and cooperation within the organisation (ENISA, 2018).

Gender may also influence employee behaviour and attitudes, as men tend to be more confident in their cybersecurity behaviour and privacy attitude online than women (Halevi et al., 2016), although women generally perceive vulnerability more and are more likely to behave securely (Hearth & Rao, 2009). Men seem to be influenced by attitudes towards technology, while women by social roles, behavioural controls, and norms (Morris et al., 2005). Hence, to instil appropriate cybersecurity culture, a gender-balanced workplace and appropriate framing of the new culture are necessary (ENISA, 2018).

COMPLIANCE AND PERSONALITY

People's behaviour may be influenced by the perceived costs and benefits of security compliance (Beautement et al, 2008), such that to persuade staff to act securely, risk

perception is key (Gonzalez & Sawicka, 2002). For achieving lasting change, people should understand: (1) the threats they are faced with; (2) the security policy they must comply with; and (3) the responsibility they carry (De Veiga & Martins, 2015).

Individuals are generally bad at evaluating the risks of cyber threats, overestimating their rarity as well as their knowledge and control over them. Various biases contribute to this, including a false sense of familiarity with cyber threats, and viewing omissions as acceptable behaviour in uncertain circumstances (ENISA, 2018).

Awareness and education programmes can be used to change risk perceptions and teach employees how to easily carry out security tasks in a confident manner (van Niekerk & von Solms, 2005a; Beautement et al, 2008). A positively framed cybersecurity programme based on openness, trust and empowerment is more likely to have a lasting impact and ensure compliance than solely relying on fear and blame (Lacey, 2010).

THE SOCIAL ENVIRONMENT

Humans are social beings that follow group norms, and it has long been known that peer pressure to conform can influence a person's behaviour. The same is true for cybersecurity behaviour.

As people want to gain the approval of others, their behaviour may be seriously influenced by the perceived expectations of managers and peers. Clear cues from management regarding the place of cybersecurity in the organisation, and the collective behaviours of co-workers can have a large impact on developing secure behaviour. A cybersecurity culture, coupled with job satisfaction and organisational support all lead to enhanced security compliance (ENISA, 2018).

Employees are also more motivated to comply with their organisation's security strategy when they believe others around them do as well (Hearth & Rao, 2009). People's tendency to follow the example of others in uncertain or new circumstances is a powerful social driver for behavioural change, which is especially true when people can openly observe and discuss security behaviours with others using the same cybersecurity tools (Das et al., 2014).

Therefore, a cybersecurity programme designed to incorporate sharing, interaction and security announcements can be effective in ensuring all employees take individual and collective responsibility for their security behaviours (Hong et al., 2015).

People naturally strive towards better outcomes for their community (Ardichvili, 2003). The belief that an individual's secure actions impact the overall security of the organisation is more likely to encourage such behaviour. This means that clear messages should be conveyed to employees regarding the importance of cybersecurity and the impact of their actions in this regard (Hearth & Rao, 2009). In the context of this study, it is perceived that an

appropriate cybersecurity culture in TVET colleges can spread to the surrounding communities.

External factor: National culture

National cultures can determine and influence individuals' values and assumptions and so shape cybersecurity culture. Specific values which are dictated by national culture include deference to authority, individualism vs. collectivism, the avoidance of uncertainty, and perceptions of control (Leidner & Kayworth, 2006). All of this can impact the development of a cybersecurity culture.

National cultures can also affect the adoption, development, distribution, and availability of technologies that naturally lead to differences. National differences in how people use specific technologies are also linked to their attitudes to privacy (ENISA, 2018).

Organisational requirements for a successful cybersecurity culture programme

Management approach

While senior buy-in is essential, the initiative to develop a cybersecurity culture can come from anywhere within an organisation. Different initiation approaches include the following (ENISA, 2018):

- **Top-down approach**: initiated by the Board, CEO and/or the most senior C-suite individual with responsibility for cybersecurity.
- **Mid-level approach**: initiated by mid-management with responsibility for cybersecurity or corporate culture (e.g. Chief Security Officer).
- **Bottom-up approach**: initiated by an individual within a business unit who identifies a need.

Creating a receptive environment

Environmental motivation comes either from the physical environment or organisational culture, in other words, from established incentives and penalties. To change behaviour, the easiest thing to do may often be to change the environment and make the desired behaviour easier to achieve. Environmental influencers reflect the design of the environment, the physical environment such as the workplace, and the technology, but also the economic factors (Bada & Sasse, 2014).

An effective cybersecurity culture should be encouraged and nurtured within the wider organisational culture in collaboration with the employees, rather than imposed if the value of cybersecurity is to be accepted by all members. Changes to the working environment in the organisation require clear responsibilities and the involvement of everyone within the

organisation, including senior management, fostering ownership of the program and the motivation to adhere to it. Commitment to cybersecurity should be signalled through sufficient budget allocation and motivation for greater security than simply compliance.

ASSEMBLING A CYBERSECURITY CULTURE TEAM

The first pre-treatment step in the process to set up a cybersecurity culture within an organisation is to assemble a cybersecurity culture team. The combination of team members is, in that regard, important as the following should be ensured (ENISA, 2018):

- The legitimacy of the approach.
- The longevity of the programme.
- That cybersecurity culture reaches all levels of the organisation.
- That the technological infrastructure is up to date and reflects the business needs of the employees.
- That the team knows what the assets are and how to protect them.
- That the team engages the employees and provides them with relevant and suitable training materials.
- That the team's approach is compliant and legal.

While the contextual reality of each organisation differs (by size, organisational structure, responsibilities attached to roles, geographical distribution, the existing culture, business sector, etc.) the successful cybersecurity culture team is typically comprised of a core set of individuals potentially accompanied by others drawn from across the organisation.

ROLES AND RESPONSIBILITIES

(ENISA, 2018)

Senior Management and a dedicated member of the board or a high-level person are responsible for championing and signalling support for cybersecurity within the organisation and ensuring adequate resources (human and financial) to set up and maintain a strong cybersecurity culture.

IT Department should contribute expertise in cybersecurity and ensure up-to-date technical measures, which are effective, simple, and useful in supporting secure behaviour without being burdensome. Cybersecurity expertise should be a core competency in the IT department and should be used as input for risk management, offering insights to senior management and supporting decision-making.

Cybersecurity professionals should help with their expertise in cybersecurity, good security governance, people, and progress management. They also should have a crucial role in the working group, to align IT and security goals, participate in the drafting of the cybersecurity strategy and policy and represent cybersecurity at the executive level.

Human Resources (HR) should provide a connection from management to the employees and oversee all staff-facing practices such as awareness-raising, training and communication. HR also brings to the table knowledge and insight into the behaviour of staff, and their different roles and knows how to embed new practices within already established processes. HR can ensure that everyone goes through the same training and can oversee any evaluations, incentive schemes or disciplinary sanctions.

The legal department should ensure that all new practices contribute to the full compliance of the company with national and international legislation, including data protection. The legal department will also assist with defining what can be asked of employees within the remits of their contracts, and how to amend contracts if needed.

The marketing and **Communication** department/s should mind that cybersecurity culture is about changing mindsets, and perceptions and conveying knowledge to people. In that regard, the marketing and communications department/s should support the change by designing and promoting cybersecurity awareness and education programmes through developing impactful communication and ensuring effective use of messages and channels for communication.

METHODS FOR DELIVERING CYBERSECURITY CULTURE PROGRAMMES

Organisations use a variety of methods to deliver cybersecurity messages and training to employees. Online methods, as well as offline and hybrid methods, are useable for raising cybersecurity awareness amongst employees when creating a strong cybersecurity culture. The method for delivery of cybersecurity messages should be chosen specifically for each organisation that fits with the current culture and methods of communicating (ENISA, 2018):

ONLINE

Emails are an easy way of reaching everyone within an organisation. They can be used to deliver direct cybersecurity messages from the top (agenda setting, warnings of new threats etc), or used by HR to deliver new training materials such as videos, games, tip sheets, stories, and FAQs. Emails are also the delivery tool for simulating phishing attacks, which will raise the awareness of employees.

Videos can be used for training and awareness-raising purposes. They can also feature stories of good practice to demonstrate the value of a correct response to a cyber threat. Videos can also feature talks by internal or external experts or employees with cybersecurity responsibilities.

Games are increasingly used for training and education and cybersecurity is no different. Games and role-playing facilitate engagement, participation, and openness.

Webinars featuring internal or external experts are an interactive a cost-effective way to deliver cybersecurity messages to employees. The webinars can also be saved and presented

in an accessible place (e.g., the company intranet) for those employees who could not attend or to re-visit aspects of the talk.

Online training courses are a good way to deliver cybersecurity training. Courses can be designed as 'blanket' courses for all employees and/or specific target groups depending on organisation structure and focus.

Social media can be useful to communicate good cybersecurity habits, alert about specific threats, and refer to good practices and useful resources. For this to work well, the organisation must have strong social media practices and employees must follow its accounts.

HYBRID

Run scenarios, **rehearsals**, **sandboxes**, and **Wargaming** exercises can positively contribute to the cybersecurity culture. Scenarios/exercises with employees from one or more departments can be run to increase preparedness for cyber events, to identify previously unrealised gaps in/clashes-between processes or identify risks. Furthermore, it can increase appreciation of different units' needs, and create behaviours/responses that are produced [and owned] by the staff within the business units, rather than imposed by the security team.

Stories of **employee good practices** are an effective way to deliver relevant advice and learning material that employees can identify with. The stories can feature a response to a current threat, what measures the employee took and what the result was. Stories can be printed on flyers or posters, told in a video or during online training.

Incentives can be offered to promote 'good' behaviour and discourage 'bad' behaviour. These do not have to be large rewards (e.g., company merchandise, gift certificates, etc.). These can be linked to an individual's behaviour or the behaviour of entire business units. Competitions can be run across the business concerning the 'best performing' team/unit.

Tip sheets are short lists providing easy access to key information about cybersecurity. They are aimed at advising on response to cyber threats clearly and concisely. These can be printed in flyer form, as posters or placed online on the company intranet.

Frequently asked questions (FAQs) like tip sheets are an effective way to organise information into easily navigated text. The FAQs can be printed as flyers or posters or posted online for employees together with a search function.

'Mock attacks' are also useful for developing cybersecurity awareness. These can include online attacks in the form of fake phishing emails sent to staff, through to offline attacks whereby physical access controls. Entry to building procedures, visibly wearing the correct pass, and alike, are tested using fake staff, or fake CEO fraud phone calls - these are undertaken to test adherence to correct processes and procedures.

OFFLINE

1-to-1 or group training sessions, as with workshops, these sessions are a good way to provide an interactive learning environment, where employees can learn, test their skills, make mistakes, and ask questions in a safe environment. While group training sessions can deliver the training for all employees, 1-to-1 sessions can deliver a targeted message for specific individuals that may have specific responsibilities concerning cybersecurity.

Flyers, like posters, can be effective at delivering short and easily digested cybersecurity information and advice. They can also feature tips, FAQs, short stories and contact details for the cybersecurity team. Flyers are a good way to reach both staff and others who visit organisational premises (e.g., clients and business partners) and help broaden the audience of the cybersecurity message.

Workshops allow for an interactive environment for employees to attend, receive training/information and are also able to ask questions. To play around with different formats and focus, internal and external speakers can be invited. For this, a supportive and positive environment so employees feel safe to ask questions and make mistakes should be ensured.

Events focusing on general cybersecurity, a specific threat, and tools against cybercrime allow for a more informal approach where people can attend talks, take-home printed materials or cybersecurity merchandise. These could be extended to the families of employees, business partners and clients.

External expert lectures are a good opportunity to get a broad and up-to-date understanding of cybersecurity issues and trends.

Posters can be used for a variety of purposes to highlight cybersecurity within an organisation. Posters can feature advice, tips on good resources, an overview of threats, presenting new threats, providing advice and contact details etc.

MEASURING CYBERSECURITY CULTURE PROGRAMMES

While the role of cultivating a culture in pursuing cybersecurity is well-appreciated, research focusing intensely on defining and measuring cybersecurity culture is still in its infancy (da Veiga, 2016). However, due to the relationship between information security and cybersecurity, it is reasonable to assume that what describes an information security culture should also apply to the cybersecurity culture (Reid & van Niekerk, 2014; Gcaza, N. & von Solms, R. (2017a).

Cybersecurity culture metrics serve the purpose of measuring security culture. They are not measuring awareness training completion rates or phishing assessments. Cybersecurity culture metrics measure the sentiments towards security in an organisation – the psychological and social aspects that drive individual and social behaviour (Laycock et al., 2019).

A measurement of a cybersecurity culture is needed to change or direct the culture of different population groups, for example, children at a specific school, employees of a company, or citizens in a certain region. This will aid in identifying the concepts of cybersecurity ("what") and "how" to educate communities to foster a cybersecurity culture that upholds ethical, security, and privacy principles (da Vega, 2016).

In the context of this study, it is important to measure and assess the change in cybersecurity culture in TVET colleges and possibly the communities surrounding these institutions of higher learning.

The future cybersecurity culture programmes' impact cannot be quantified if the current situation level of the target is not established first. This holds whether we are focussing on the entire organisation or specific business units/demographics within the organisation.

Approaches and guidance on selecting appropriate metrics are presented below (ENISA, 2018). In other words, three different approaches can be employed by an organisation to produce a pre-treatment cybersecurity culture current situation before they implement their selected programmes: (1) to measure cybersecurity culture separately from the treatments employed, (2) the second is to use the selected metrics of the treatments as the current situation, (3) to conduct both approaches together. All three approaches are employed within organisations that have actively developed cybersecurity programmes.

APPROACH 1: DETERMINE A CYBERSECURITY CULTURE CURRENT SITUATION INDEPENDENTLY FROM THE CYBERSECURITY CULTURE INTERVENTIONS

Using this approach, calculating a current situation measurement or cybersecurity culture 'score' for the organisation is achieved by conceptualising cybersecurity culture as one or more dimensions to be measured via a data collection process. This cybersecurity culture score is determined separately from the interventions, hence is not a step included in the step-by-step implementation guide for cybersecurity culture programmes in Section 2 (it would occur early in the pre-treatment phase). This approach employs the following process:

- *Step 1*: Collect data from/on the staff relating to aspects of behaviour, attitudes, awareness, etc., and calculate a current cybersecurity culture situation.
- *Step 2*: Develop and implement the cybersecurity culture interventions, employing the eight-step Implementation Framework In Figure 7.
- *Step 3*: Re-measure the cybersecurity culture's current situation at future intervals to determine changes in the organisational cybersecurity culture levels.

Determining the cybersecurity culture's current situation requires either developing an in-house methodology for conceptualising and calculating cybersecurity culture or using external consultants and/or off-the-shelf products to achieve this.

One off-the-shelf example is the Security CLTRe Toolkit (Laycock et al., 2019) which breaks cybersecurity culture into seven dimensions, measured by a staff questionnaire. These dimensions constitute metrics, with the analysis of the collected data providing the organisation's security culture score, both as an overall total and values for each dimension that can be mapped on a spider graph. The seven metrics employed to measure cybersecurity culture within the Security CLTRe Toolkit are presented in Table 3.

Table 3: CTRLe's seven dimensions for measuring CSC (source: Laycock et al., 2019)

Behaviours: Actual or intended activities and risk-taking actions of employees that have direct or indirect impact on security culture
Attitudes: Employees' feelings and emotions about the various activities that pertain to organizational security
Cognitions: Employees awareness, verifiable knowledge and beliefs regarding practices, activities and self-efficacy that are related to organizational security
Compliance: Adherence to organizational security policies, awareness of the existence of such policies and the ability to recall the substance of such policies
Communication: Ways employees communicate with each other, sense of belonging, support for security issues and incident reporting
Norms: Perceptions of what sort of security-related organizational conduct and practices are deemed normal by employees and their peers and what practices are informally perceived as deviant
Responsibilities: Awareness of the importance of every employee as a critical factor in sustaining or endangering the security of the organisation

Benefits: This approach provides an overall cybersecurity culture picture/value for the organisation and/or business units enabling the plotting of shifts in cybersecurity culture over time. Additionally, multiple organisations and/or business units employing the same standardised cybersecurity culture measuring instrument enables comparisons both between and within organisations, and the ranking of businesses/units – hence the cybersecurity culture implementation team will be able to identify stronger and weaker areas within their business for the targeting of resources and programmes.

Drawbacks: This approach does not negate the need to develop additional metrics for individual cybersecurity culture treatments – i.e., it is still needed to undertake pre- and post-treatment measurements with appropriately selected metrics for each cybersecurity culture programme implemented, otherwise it cannot be determined the effect of individual programmes. In addition, measurement tools based solely on self-completion questionnaires are affected by numerous biases (e.g. selective-reporting bias, providing desirable responses over reality, question patterns, etc.). While questionnaire designers/administrators can employ techniques to minimise these effects, they cannot be completely mitigated. Finally, positive, or negative correlations between overall cybersecurity culture scores and the effects of cybersecurity culture treatments do not imply causality.

APPROACH 2: DETERMINE A CSC'S CURRENT SITUATION BY UTILISING THE CYBERSECURITY CULTURE'S CURRENT INTERVENTION METRICS

Using this approach, developing the cybersecurity culture's current situation should be a part of the step-by-step implementation guide by taking the results of the pre-treatment metrics and using these as the cybersecurity culture's current situation. This approach uses the physical manifestation of cybersecurity-relevant activities of staff as the cybersecurity culture's current situation of that organisation. This entails the following steps:

Step 1: Create a list of metrics relevant to the cyber security activities of the organisation.

Step 2: Calculate pre-treatment values of these metrics through whatever data collection methods are most appropriate. These values constitute the current cybersecurity culture situation.

Step 3: Develop and implement the cybersecurity culture interventions, employing the eight-step Implementation Framework (Figure 7).

Step 4: Re-measure these metrics by calculating their post-treatment values to determine any changes in the organisational cybersecurity culture levels.

Here is an example of applying Approach 2. To produce their cybersecurity culture baseline, the implementation team at Acme Inc. begin by brainstorming a list of relevant metrics. A few examples from their wider list include the following:

- Desks clear of confidential documents at end of the day.
- Employees' [virtual] desktops are logged off when not at a desk.
- Not clicking on links from untrusted external sources.
- Following reporting procedures for suspicious cyber activities.

Having created their list of metrics, the cybersecurity culture implementation team identified appropriate measurement methods:

- Desks clear of confidential documents at end of the day: physical inspection by security staff or team leader.
- Employee's [virtual] desktops logged off when not at desk: log files.
- Not clicking on links from untrusted external sources: employ fake phishing emails.
- Following reporting procedure for suspicious cyber activities: employ an attack drill or conduct an online knowledge test of the reporting procedure.

Before developing and implementing any cybersecurity culture programmes targeting these metrics the implementation team should conduct pre-treatment measurements of these metrics – the results of which constitute Acme Inc's CSC baseline (ENISA, 2018).

Benefits: By selecting metrics based on specific behaviours, and then conducting pre- and post-treatment measurements, it is easier for the cybersecurity culture implementation team to demonstrate the causal effect of their treatment programmes. Consequently, this enables the modification of future programmes based on the results and demonstrated impacts that can be leveraged for greater resource allocation. The list of metrics comprising the cybersecurity culture's current situation can be tailored to reflect the specific context and make-up of an organisation. Additionally, by employing the same measuring methods across an organisation, the results of different business units and/or sub-sets of employees can be compared by the cybersecurity culture implementation team to identify stronger and weaker groups for the tailoring of future treatments.

Drawbacks: This approach reduces cybersecurity culture to the specific behaviours covered by the selected metrics, and given the wide scope of behaviours, norms, beliefs, attitudes, end alike, that comprise cybersecurity culture. This cybersecurity culture current situation is likely to represent only a subset of the wider cybersecurity culture within an organisation. The bespoke nature of this approach prevents standardised comparisons of current cybersecurity culture situations between different organisations, making it harder to identify how one organisation compares to others in a similar space.

APPROACH 3: COMBINE APPROACHES 1 AND 2

Given that (a) both two previous approaches possess unique benefits, and (b) many of the drawbacks of each approach are addressed by the other, the cybersecurity culture implementation team may choose to employ both approaches. If this third, combined approach is adopted, the cybersecurity culture team may select to measure the overall score (as outlined in approach 1) periodically (e.g., annually, bi-annually, etc.) to provide a higher-level picture of the organisation's cybersecurity culture, while measuring specific behaviours as part of the ongoing cybersecurity culture activities (as outline in approach 2).

'GOOD' VERSUS 'BAD' METRICS FOR MEASURING SUCCESS

Metrics are necessary for both establishing the cybersecurity culture's current situation and measuring the impact of the cybersecurity culture programmes. When selecting such metrics, organisations already recognise the need to utilise those that are relevant to both the context of their organisation and their organisation's cybersecurity goals. However, aside from any contextual requirements, cybersecurity culture implementation teams need to appreciate that not all metrics that measure cybersecurity can be utilised to measure cybersecurity culture. In this respect, for the specific purpose of measuring cybersecurity culture, there are both 'good' and 'bad' metrics:

- A good cybersecurity culture metric tells the implementer something of value about the culture of cybersecurity within an organisation.

- A bad cybersecurity culture metric does not provide the implementer with valuable information about the organisation's cybersecurity culture regardless of whether it pertains to cybersecurity.

Here are some good and bad metrics examples in practice. It is accepted good practice that organisations should have a cyber security policy, but such policies can only impart value if employees are familiar with its content. As a result, the ISO at Acme Inc. conducts an online training programme to familiarise employees with the policy. The aim was to measure the awareness impact of this programme which requires selecting a suitable metric.

- A poor metric here would be to measure the number of employees who undertook the training. While this is quantifiable it provides no information of value on how aware employees are of the actual content of Acme's cyber security policy.
- A good metric would be to test employees' knowledge of the content of this policy by conducting pre- and post-testing on either side of the online training programme, as the data collected pertains directly to the CSC of Acme Inc. (ENISA, 2018).

This research developed its metrics following the constructed Conceptual implementation model for developing cybersecurity culture at TVET colleges (Figure 8) and uses the variables, coming from the qualitative survey questions, given in Appendix C.

CHAPTER 4: CYBERSECURITY CULTURE IMPLEMENTATION CONCEPTUAL MODEL

Any model, including the one devised by this study, starts with the definition of a cybersecurity culture. This research adopted the definition of cybersecurity culture as the promotion of cybersecurity practices that integrate seamlessly with people's work and life. It means making people aware and knowledgeable of cybersecurity threats and causing them to amend their behaviour accordingly to mitigate potential threats. Cultivating cybersecurity is an apt approach to promote a secure consumption of cyberspace, aimed at instilling a certain way of "naturally behaving" in daily life, a way that subscribes to certain cybersecurity assumptions (Wamala, 2011; Gcaza et al., 2015).

The reviewed literature provided the major categories of the cybersecurity culture that are used for creating the "Conceptual implementation model for developing cybersecurity culture at TVET colleges" (Figure 8). This model consists of eight categories: (1) Dimensions, (2) Layers, (3) Factors, (4) Practices, (5) Implementation strategy and guidelines, (6) Education and training (7) Forms of delivery, and (8) Measuring cybersecurity culture, including monitoring and evaluation.

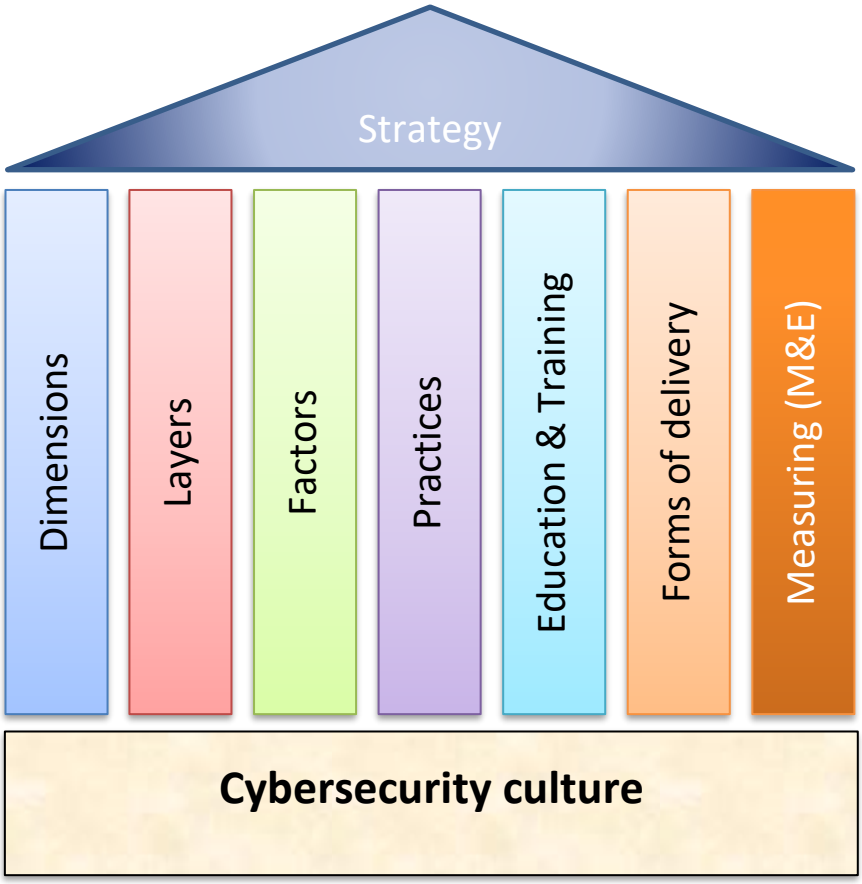

Figure 8: Conceptual implementation model for developing cybersecurity culture at TVET colleges (source: Authors)

The categories are divided into components, and elements or factors. The further text in this chapter describes these categories through the belonging elements and factors.

DIMENSIONS OF CYBERSECURITY CULTURE

The dimensions of cybersecurity culture, according to the reviewed literature, include the following components: (1) Attitudes, (2) Cognition, (3) Communication, (4) Compliance, (5) Norms, and (6) Responsibilities.

ATTITUDES

This component suggests that it is essential to generate and maintain the positive attitude of TVET teachers, students, and managers towards digital technology and encourage their readiness and ability to use digital teaching and learning methods as well as to secure teaching and learning material and processes (Bandara et al., 2014; Lange, Hofmann & Di Cara, 2020). Attitudes also relate to the feelings and beliefs that the TVET colleges teachers, students, and managers have toward the cybersecurity protocols and issues. Attitudes are commonly expressed in terms such as prefer, like, dislike, hate, and love and involve a preference for or against something.

Social psychology has discovered that attitudes are made up of cognitive, affective, and behavioural elements (Jhangiani et al, 2014). Here are illustrative examples related to the answers of the surveyed TVET colleges' teachers, students, and managers:

- In terms of **affect**: They feel happy when they use modern ICT.
- In terms of **cognition**: They are not fully cognisant regarding possible cyber-attacks and ensuing damages.
- In terms of **behaviour**: Consequently, they do not regularly update their devices.

The behaviour relates to the actions and activities of teachers, students, and managers that have a direct or indirect impact on cybersecurity. For example, there are different types of users (teachers, students, managers, and other staff) and many of them behave in a non-malicious way. However, these users have low simple technical knowledge related to, for instance, password creation and sharing (Stanton et al, 2005; Sandler, 2018).

Opposite of these non-intentional actions are so-called "deviant behaviour". This type of behaviour describes those actions which are intentional and are often labelled as sabotage, stealing, and industrial or political espionage (Crossler et al., 2013).

COGNITION

This component corresponds to the teachers, students, and managers' understanding, knowledge and awareness of cybersecurity issues and activities.

According to the created Conceptual implementation model for developing cybersecurity culture at TVET colleges model, the acquisition of knowledge for cybersecurity culture is achieved through awareness training and education (ENISA, 2010). In general, these activities are expected to:

- **Communicate** cybersecurity **knowledge** (i.e. recommended guidelines and security best practices) to the target audience.
- **Broaden** the cybersecurity **knowledge** of the target audience (i.e. familiarity with guidelines and security best practices), hence…
- **Bring positive changes** in **attitude** (i.e., motivate to adopt recommended guidelines and practices) and behaviour (i.e., create a strong culture of cybersecurity) in the target audience, i.e., the TVET colleges' teachers, managers, and students.

Hence, cybersecurity culture-related awareness programmes should be devised and provided for all stakeholders in TVET colleges (teachers, students, managers, and the admin staff).

COMMUNICATION

Communication component of the cybersecurity culture Dimensions can play a vital role in maintaining cybersecurity at TVET colleges. It is a mechanism for securing or compromising information through the management of people and technology (Backhouse & Dhillon, 1996; Arhin & Wiredu, 2018). This relates to the quality of communication channels for discussing security-related events, promoting a sense of belonging, and providing support for cybersecurity issues and incident reporting at TVET colleges.

COMPLIANCE

The compliance component refers to knowledge of written cybersecurity policies and the extent that people follow them. Cybersecurity compliance ensures that security mechanisms implemented in TVET colleges work together effectively to protect critical information and digital devices (Kim et al., 2016). The adoption of cybersecurity compliance in TVET colleges will involve (Al-Kalbani et al., 2017):

- Implementation of **effective** and **balanced cybersecurity measures** and **mechanisms**.
- **Compliance** with **legal** and **cybersecurity requirements** and expectations of the colleges.
- **Maintaining** teachers', students, and managers (also the admin staff) **confidence** and **trust** in cybersecurity.

NORMS

Norms are typically understood to be one of the most important mechanisms that influence humans**,** thus a key element of a cybersecurity culture. Sociological, socio-psychological, and behavioural cybersecurity researchers suggest that the Norms component will guide TVET

colleges teachers, students, and managers in their use of institutional information systems and will highlight norms as one of the key elements that characterise their cybersecurity behaviour and compliance **(**Hechter & Opp, 2001; Siponenet al, 2010); Laycock et al, 2019). These are general characteristics or requirements for cybersecurity norms (IGF, 2018):

- Be **easy** to **understand** and **abide** by.
- Provide **clarity** of the **potential** cybersecurity **risks** and "**best practices**" to follow.
- Provide proper **support** through **training** to abide by the norms.
- **Create awareness** of the **legal provisions** against cybercrime.
- **Foresee regular updates**: (1) at the technical level (patches, updates, etc.) to protect oneself and (2) information on the latest developments including global "best practices".

RESPONSIBILITIES

This notion relates to how the TVET colleges' teachers, student, and managers perceive their role as a critical factor in sustaining or endangering the cybersecurity of the organisation. In other words, the Responsibility component is mainly related to their practices and performances such as monitoring and control, reward and deterrence and acceptance of responsibility (Al-Hogail, 2017).

LAYERS OF CYBERSECURITY CULTURE

According to this category, organisational culture is viewed as manifested in three layers: (1) tacit assumptions that are beliefs about reality and human nature; (2) espoused values, which refer to social principles, philosophies, goals, and standards; and (3) artefacts that are visible, tangible, and audible results of activity grounded in values and assumptions (Hatch, 1993).

TACTIC ASSUMPTIONS

Viewing cybersecurity as an integral part of conducting teaching and learning at TVET colleges is important for avoiding contradictory narratives in the institution that can reduce the effectiveness of cybersecurity roles and measures. If teachers, students, and managers view cybersecurity as integral to business at the college, it is likely to strive for a balance between cybersecurity goals and goals of teaching and learning. Cybersecurity is both an organisational and technical issue but also a tactic issue, including the view of whether cybersecurity is static or dynamic (Reegård et al, 2019).

ESPOUSED VALUES

The assumptions matter as these are linked to the espoused values and the rationale of the institution in how to best manage cybersecurity and cybersecurity culture (Barton et al, 2016; Al-Izki & Weir, 2016). Whether cybersecurity is seen as a responsibility of the whole institution or specific parts of it (i.e. teachers, managers, and students) also represents value. An example is the issue when technical personnel are left to manage cybersecurity in isolation.

For instance, if the person in charge of cybersecurity struggles between contradictory pulls in the institution, that rendered their role and efforts in cybersecurity less effective by needing to seek constant buy-in from teachers, managers, and students (also other stakeholders (Ashenden & Sasse, 2013).

ARTEFACTS

The beliefs and values of the institution about cybersecurity translate into observable behaviour and practices or non-practices (Reegård et al, 2019). The top management's active participation, championing and/or financing of cybersecurity activities are, for example, the most mentioned in the pertinent literature. Cybersecurity awareness and training programs and cybersecurity policies are also well-known artefacts of cybersecurity culture (e.g. Ashenden & Weir, 2016; Steinbart et al, 2018).

The layers of cybersecurity culture are interconnected and understanding each may be necessary for ensuring the implementation of adequate measures (Van Niekerk & von Solms 2010). For example, understanding the values that drive people's actions can contribute to a greater understanding of compliance issues with cybersecurity policies (Hedström et al, 2011).

FACTORS IMPACTING CYBERSECURITY CULTURE

The elements of this category, i.e. factors that can impact cybersecurity culture are divided into four groups: Organisational factors (organisational culture, the institution's wider cybersecurity strategy, cross-institutional commitment), Human factors (psychological factors, compliance and personality), Social environment (creating a receptive environment), and External factors (national culture).

ORGANISATIONAL FACTORS

Organisational culture

Organisational culture can reinforce the commitment to the organisation and enhance stability by offering guidance and accepted standards for employee behaviour. Both acceptable and unacceptable behaviour should be defined in line with the organisation's wishes and encouraged or denounced respectively. If sanctions are enforced, consistency in their application is needed to ensure compliance and influence changes in the mindsets of people (Alnatheer et al., 2012).

Against this backdrop, an effective cybersecurity culture programme, based on the conceptual model derived from this study, should be fully embedded within the TVET colleges' culture if the value of cybersecurity is to be accepted by all – primarily the teachers, managers, and students engaged in this study. A commitment to cybersecurity will support a wider institutional culture of excellence (RAND, 2008).

The institution's wider cybersecurity strategy

A successful strategy should: (1) reinforce strong governance attitudes and actions; (2) be designed similarly to other business functions (primarily teaching and learning in the context of this study) to ease acceptance; (3) be built around an adaptable framework to facilitate long use; and (4) its effectiveness should be measurable to demonstrate success (ENISA, 2018). Regarding this study, this can only be advised by the colleges' management but cannot be enforced.

Cross-institutional commitment

The cross-institutional commitments translate into the roles to be played by the following different groups:

THE ROLE OF SENIOR MANAGEMENT

Beginning, transmitting, and embedding cultural change requires leadership and buy-in by senior management, and to ensure this change is lasting, it should signal its commitment and involvement in cybersecurity culture by allocating sufficient resources for comprehensive programmes while delegating clear responsibilities and authority (Alnatheer et al., 2012).

THE ROLE OF THE PEOPLE CHARGED WITH ENSURING CYBERSECURITY

These people have a crucial role in developing a cybersecurity culture. They must understand the needs and operations while using their technical and communication skills to align IT and cybersecurity goals with business ones - teaching and learning in the case of this study. These people should participate in drafting the cybersecurity strategy and represent security at the executive level while maintaining good communication channels with both senior management and the targeted populations to effectively share their vision (Ashenden, 2008).

THE ROLE OF MIDDLE MANAGEMENT (TEACHERS)

As the intermediary between employees and senior management, middle management has a key role to play in setting the tone of cybersecurity in an organisation. They need to be convinced of its benefits and should be effectively involved in the implementation of cybersecurity throughout the organisation. In the context of this study, the role of middle management should be assumed by the IT and other teachers at the TVET colleges.

THE ROLE OF THE IT DEPARTMENT

The role of the IT team in cybersecurity culture is multifaceted. The team should ensure that up-to-date technical measures are adopted, which are effective, simple, useful and support secure behaviour by not being overly burdensome. To effectively achieve these aims by tailoring solutions, those maintaining the technical infrastructure must understand the structure of their organisation and its activities to further guide the cybersecurity programme (RSA, 2017).

THE ROLE OF THE LEGAL/COMPLIANCE DEPARTMENT

The legal/compliance department has a role to play by offering expert legal advice to ensure any cybersecurity culture and cybersecurity practices embedded in the organisation comply with national and international legislation, including data protection norms such as POPIA. The department should also provide support when designing the cybersecurity culture curriculum.

THE ROLE OF HUMAN RESOURCES

Human resources (HR) have an important role as a connector between management and employees – the teachers, managers, and admin staff, in the context of this study. Thanks to their position within an organisation, HR can offer insights into the behaviour and psyche of employees, which in turn can be used to counter potential insider threats or design and deliver effective security education programmes. The department can also ensure that everyone in the institution undergoes the necessary cybersecurity training by enforcing compliance while conducting cybersecurity practice evaluations of employees and, where necessary, enacting disciplinary sanctions (ENISA, 2018).

THE ROLE OF THE MARKETING/INTERNAL COMMUNICATIONS DEPARTMENT/S

Cybersecurity culture is about changing mindsets and perceptions, and conveying knowledge to people, with security presented to employees as 'business as usual'. The marketing department can assist the cybersecurity culture development by designing and promoting security awareness and education programmes and producing messaging that maximises impact and emphasise the benefits of a cybersecurity culture. They can also maximise cost-effectiveness by leveraging personalised approaches and multiple channels (Bernik et al, 2008).

HUMAN FACTORS IN CYBERSECURITY CULTURE

Psychological factors

To convince people to change, three parallel processes must take place: (1) there must be dissatisfaction with the current situation, (2) this dissatisfaction must cause anxiety and/or guilt, and (3) people must be able to adopt new behaviour in a safe environment without compromising their identity or integrity (Schein, 2004).

Compliance and personality

People's behaviour may be influenced by the perceived costs and benefits of cybersecurity compliance (Beautement et al, 2008), such as to persuade people to act securely, risk perception is key (Gonzalez & Sawicka, 2002). For achieving lasting change, people should understand: (1) the threats they are faced with; (2) the security policy they must comply with; and (3) the responsibility they carry (De Veiga & Martins, 2015).

SOCIAL ENVIRONMENT

Humans are social beings that follow group norms, and it has long been known that peer pressure to conform can influence a person's behaviour. The same is true for cybersecurity behaviour.

As people want to gain the approval of others, their behaviour may be seriously influenced by the perceived expectations of managers and peers. Translated from the ENISA (2018) document into this study, a clear cue from managers to teachers and then from teachers to students regarding the place of cybersecurity at TVET colleges and the collective behaviours can have a large impact on developing cybersecurity behaviour. A cybersecurity culture, coupled with job satisfaction of managers and teachers and institutional support all lead to enhanced cybersecurity compliance.

Creating a receptive environment

Environmental motivation comes either from the physical environment or organisational culture, in other words, from established incentives and penalties. To change behaviour, the easiest thing to do may often be to change the environment and make the desired behaviour easier to achieve. Environmental influencers reflect the design of the environment, the physical environment such as the workplace, and the technology, but also the economic factors (Bada & Sasse, 2014).

An effective cybersecurity culture should be encouraged and nurtured within the wider organisational culture in collaboration with all people, rather than imposed if the value of cybersecurity is to be accepted by all stakeholders. Changes to the working environment in an organisation require clear responsibilities and the involvement of everyone within the organisation, including senior management, fostering ownership of the program and the motivation to adhere to it. This implies the involvement of all stakeholders at TVET colleges in building an effective cybersecurity culture.

EXTERNAL FACTOR: NATIONAL CULTURE

National cultures can determine and influence individuals' values and assumptions and so shape cybersecurity culture and ICT use in general. Specific values which are dictated by national culture include deference to authority, individualism vs. collectivism, the avoidance of uncertainty, and perceptions of control (Leidner & Kayworth, 2006). All of this can impact the cybersecurity culture development.

We are aware that this research cannot change this variable, but the result of this research might prompt national policymakers to integrate cybersecurity culture into the national culture. This could be one of changing factors of the all-over national culture in this, technology-driven fast-changing world.

CYBERSECURITY CULTURE PRACTICES

These are the following main cybersecurity practices recommended by the reviewed literature: (1) Management support, (2) Cybersecurity policies, (3) Involvement and communication, and (4) Learning from experience.

MANAGEMENT SUPPORT

Management support can come in a variety of forms. It ranges from a willingness to financially invest in initiatives and advocate for cybersecurity, to the organisation of the cybersecurity function and follow-up on cybersecurity work and status.

This kind of support is vital for creating and maintaining a focus on cybersecurity and heavily influential on the performance of other cybersecurity practices. For example, active participation and visible support by top management are of major importance to the formulation and implementation of information security policies (Karyada et al, 2005).

While senior buy-in is essential, the initiative to develop a cybersecurity culture can come from anywhere within an institution. Different initiation approaches include the following (ENISA, 2018):

- **Top-down approach**: Initiated by the Board, CEO and/or the most senior C-suite individual with responsibility for cyber security.
- **Mid-level approach**: Initiated by mid-management with responsibility for cyber security or corporate culture (e.g. cybersecurity managers).
- **Bottom-up approach**: Initiated by an individual within an institution's unit that identifies cybersecurity needs.

In the case of this study, the initiative should come from TVET colleges' managers and teachers, which will need support from the institution's top management - but also from other organisations such as INSETA or DUT.

CYBERSECURITY POLICY

Cybersecurity policies provide overall guidance in building a cybersecurity culture (Knapp et al. 2009). As that cybersecurity culture is a management issue, one of the key practices is to establish an internal policy to demonstrate management intent and the importance of cybersecurity. In devising cybersecurity policies, it is important to find a balance between the management and teachers' and students' perspectives to make such policies useful.

Documented best practices and formal policies shared throughout the institution can aid end-users of ICT and improve security. Due to a growing understanding that cybersecurity needs to be addressed also through organisational measures (education and policy) and not solely by technical measures, cybersecurity culture is attracting increasing attention (Reegård et al., 2019).

INVOLVEMENT AND COMMUNICATION

In their own work experience, end-users (in this case teachers and students) can identify information security issues as they emerge and creatively address them based on their work experiences and knowledge (Lin and Wittmer, 2017). In this way, the TVET teachers and students will have the potential to positively contribute to cybersecurity if their participation is encouraged – and, in turn, this will promote proactivity.

One of the best ways to improve motivation is through broad horizontal participation, i.e. peer-to-peer participation (Ruighaver et al, 2007). This will require genuine multi-way communication between managers, teachers, and students (including other stakeholders), negotiation and involvement to overcome the often observed 'them' and 'us' relationship (Ashenden & Sasse, 2013).

LEARNING FROM EXPERIENCE

Monitoring of specific outcomes is used to validate or falsify current beliefs regarding institutional cybersecurity (Kearney & Kruger, 2016). Auditing is another example of such a mechanism that can help in increasing the institutional awareness of its internal cybersecurity environment (Reegård et al, 2019). On the other hand, institutions may fall into a trap of an external focus when having an external audit in which the organisation is primarily focused on passing the audit rather than achieving the security they need (Ruighaver et al, 2007).

CYBERSECURITY CULTURE STRATEGY

The cybersecurity culture strategy category consists of several elements or steps: (1) Strategy direction, (2) Environmental assessment, (3) Strategy formulation, (4) Strategy implementation, and (5) Strategy control.

STRATEGY DIRECTION

The strategic direction can be derived from the long-term objectives of the institution. In the case of this study, the strategic direction is derived from: (1) the general government guidelines of the need for improving the national cybersecurity culture (SA Government Gazette, 2015) and (2) the suggestion of da Vega et al (2016) that individual and organisational cybersecurity culture can improve national cybersecurity culture.

ENVIRONMENTAL ASSESSMENT

The environmental-assessment process consists of the gathering and analysing of information, and then using the analysed intelligence in strategic decision-making. When conducting an environmental assessment, information can be gathered from different sources: personal and impersonal (also known as written sources).

In the case of this study, environmental assessment, as well as the status quo of the cybersecurity culture was tested at the two selected TVET colleges: Elangeni and Umfolozi.

STRATEGY FORMULATION

The strategy formulation process consists of three sub-processes:

- *Diagnosis*: This stems from the environmental assessment.
- *Guiding policies*: The guiding policies and coherent actions are extrapolated from the existing cybersecurity implementations. In the case of this study, the elements of the conceptual model derived from this study are used as the guiding principles.
- *Coherent actions*: This is guided by the environmental and the status quo assessments to ensure the applicability and suitability of the recommendations.

STRATEGY IMPLEMENTATION

Most strategies fail to be implemented due to the challenges and complexities of strategy implementation (Rumelt, 2011). Hence, before the process of implementing strategy, it is important to ask the following questions (Wheelen & Hunger, 2012):

1. Who are the people who will implement the strategy?
2. What needs to be done to implement the strategy?
3. How is everyone going to work together to do what is needed?

Accordingly, these questions are posed to the researched TVET college management as well as the teachers. The answers are then considered for designing the implementation (action) guidelines for the second phase (Action research) of this study.

STRATEGY CONTROL

Strategy control is intended to ensure that the stipulated strategic objectives are achieved through five steps (Goldman & Nieuwenhuizen, 2006; Enz, 2009; Wheelen & Hunger, 2012):

1. *Determine what to measure*: this will be done before the second phase of this study starts as the same measures will be implemented at the end of the intervention.
2. *Establish standards of performance*: this will be done together with the previous.
3. *Measure the actual performance*: the performance will be measured at the end of the intervention.
4. *Compare the actual performance with the established standard*: this will be done at the end of the intervention as a part of the summative evaluation.
5. *Take corrective action*, if necessary.

GUIDELINES FOR IMPLEMENTATION OF CYBERSECURITY CULTURE

This element of the cybersecurity culture conceptual model is intertwined with the cybersecurity culture strategy, which is explained in the previous section. The ENISA Framework, which is adopted by this study, is centred on specific activities, their implementation and measurement of impact, which allows for considering and amending initial goals and/or the target audience (ENISA, 2018).

Step 1: Set up the core cybersecurity culture work group.

Step 2: Business understanding and risk assessment.

Step 3: Define main goals, success criteria and target audiences.

Step 4: Calculate the current situation and do a gap analysis between the current situation and the goals.

Step 5: Select one or more activities.

Step 6: Run your selected activity.

Step 7: Rerun the current situation metric and analyse the results.

Step 8: Review and consider your results before deciding on the next action.

The implementation guidelines for this particular study will be given in the chapter describing the Actin plan for developing cybersecurity culture at TVET colleges.

IMPROVING CYBERSECURITY CULTURE THROUGH EDUCATION: CYBERSECURITY CULTURE CURRICULUM

Technology alone cannot be a cushion against cyber threats, instead, humans should occupy centre stage through cybersecurity culture (Gcaza, et al, 2015). There are a large number of works that show the usefulness of cybersecurity awareness and skills training as well as developing cybersecurity culture (e.g. Ernst & Young, 2017; Shouhuai, 2018; Huda, 2019; Beveridge, 2020).

In this study, it is envisaged that cybersecurity culture-related awareness and training should be done through the curriculum, and implemented through IT education at TVET colleges. The viability of this approach is tested through interviews with the IT teachers at TVET colleges and is described in the chapter dedicated to the verification of the Conceptual model.

CYBERSECURITY CULTURE CURRICULUM

Education occurs through the implementation and enforcement of policies and procedures. With cyberspace being such a critical component of almost all organisations, it is necessary to describe acceptable uses and responsibilities explicitly (Kavak et al, 2021). In that regard, collaborative learning experiences are normally designed and implemented with pedagogical principles in mind, whilst cybersecurity issues are largely ignored.

This may lead to undesirable situations that have a detrimental impact on the learning process, its management and learning material (Bandara et al., 2014). Hence, it was desirable to agree on the curriculum topic with the IT teachers and other relevant stakeholders such are academic advisors.

The main topics for a curriculum

The main topics for the syllabus, as proposed by Malyuk & Milosavskaya (2016) include:

- The strategy of information society development.
- Information culture and ethics.
- Information support of public policies.
- Information and psychological security, psycho-physical effects on the individual and society, and information weapons.
- The Internet and freedom of speech and protection from malicious content.
- Social challenges of the information society and the problems of education and training.
- Legal issues of information society development and protection of intellectual property: it is important to educate youth regarding not committing cybercrime as its low consequences, particularly related to the Cyber Crimes Bill, signed into law by President Cyril Ramaphosa on 1 June 2021.
- The IT crime.

These topics are discussed with the relevant stakeholders mentioned above. This led to the refinement of the curriculum aimed at improving the cybersecurity culture at TTVET colleges.

While finally constructing the cybersecurity culture curriculum, it is important to consider the following factors that can seriously impact how people behave concerning cybersecurity (Metalidou et al., 2014):

- Lack of motivation.
- Lack of awareness.
- Inaccurate beliefs about behaviours or risks.
- Risky behaviour and inadequate use of technology.

Metalidou et al. (2014) suggest that cybersecurity awareness (here derived through the curriculum) is the key to mitigating cybersecurity threats caused by human weaknesses. Agreeing that awareness is an important factor in cybersecurity culture, ENISA (2010) states that, in general, a cybersecurity awareness programme is expected to:

- Bring positive changes in attitude (i.e., motivate to adopt recommended guidelines and practices) and behaviour (i.e., create a strong culture of cybersecurity) in the target audience (in this case teachers, managers, and students).
- Gain and keep the audience's trust and satisfaction (i.e. stakeholders in this study, including INSETA).
- These are supposed to minimise the number and extent of cybersecurity breaches.

To increase awareness of cybersecurity, the targeted TVET colleges must ensure that the training through education is tailored to the target population to interpret and internalise

risk-related information through the lenses of cognitive and cultural bias (Thsohou et al, 2015). Hence, Van Niekerk & Von Solms (2010) believe that it cannot be assumed that the average teacher, manager, or student has the necessary knowledge to perform his/her job in a secure manner. Thus, cybersecurity awareness training is necessary to develop appropriate cybersecurity culture.

It is also important that cybersecurity training, stipulated in the curriculum, is interesting and engaging. In that regard, Cone et al. (2007) argue that many forms of training fail because they are repeatable and do not require users to think about and apply cybersecurity concepts.

The above suggestion is also supported by the cybersecurity awareness definition: "It is an ongoing process of learning that is meaningful to recipients and delivers measurable benefits to the organisation from lasting behavioural change" (Dowd, 2016).

Although the awareness level of the technology of end-users positively affects the behaviour, there is still a gap between the user awareness levels and their respective practices and behaviour (Furnell, 2008). This gap should be filled in by an appropriate cybersecurity culture curriculum and the evaluation of the usefulness of the curriculum and the whole intervention.

FORMS OF DELIVERY

The method for delivery of cybersecurity messages should be chosen specifically for each organisation that fits with the current culture and methods of communicating (ENISA, 2018). These are general forms of delivering syllabi related to cybersecurity culture:

ONLINE

Online training courses are a good way to deliver cybersecurity training. Courses can be designed as 'blanket' courses for all and/or specific target groups.

Emails are an easy way of reaching everyone within an organisation. They can be used to deliver direct cybersecurity culture-related messages. Emails are also the delivery tool for simulating phishing attacks, which will raise the awareness of people.

Videos can be used for training and awareness-raising purposes. They can also feature stories of good practice to demonstrate the value of a correct response to a cyber threat. Videos can also feature talks by internal or external experts or employees with cybersecurity responsibilities.

Games are increasingly used for training and education and cybersecurity is no different. Games and role-playing facilitate engagement, participation, and openness.

Webinars featuring internal or external experts are an interactive a cost-effective way to deliver cybersecurity messages to people. The webinars can also be saved and presented in an accessible place (e.g., the company intranet) for those employees who could not attend or to re-visit aspects of the talk.

Social media can be useful to communicate good cybersecurity habits, alert about specific threats, and refer to good practices and useful resources. For this to work well, the organisation must have strong Social media practices and the stakeholders must follow its accounts.

OFFLINE

Several offline techniques can be used for bolstering cybersecurity culture:

1-to-1 or group training sessions – as with workshops, training sessions are a good way to provide an interactive learning environment, where people can learn, test their skills, make mistakes and ask questions in a safe environment.

Flyers, like **posters**, can be effective at delivering short and easily digested cybersecurity information and advice. They can also feature tips, FAQs, short stories and contact details for the cybersecurity team.

Workshops allow for an interactive environment for employees to attend, receive training/information and are also able to ask questions. Workshops also allow for playing around with different formats and focus by inviting internal and external speakers.

Events focusing on general cybersecurity, a specific threat, and tools against cybercrime allow for a more informal approach where people can attend talks and take home printed materials or cybersecurity merchandise.

External expert lectures are a good opportunity to get a broad and up-to-date understanding of cybersecurity issues and trends.

Posters can be used for a variety of purposes to highlight cybersecurity within an organisation. Posters can feature advice, tips on good resources, an overview of threats, presenting new threats, providing advice and contact details, etc.

HYBRID

This method includes a combination of online and offline methods.

MEASURING CYBERSECURITY CULTURE PROGRAMMES

Cybersecurity culture metrics serve the purpose of measuring security culture. They are not measuring awareness training completion rates or phishing assessments. Security culture metrics **measure** the **sentiments towards cybersecurity** in an organisation – the **psychological** and **social** aspects that **drive individual** and **social behaviour** (Laycock et al., 2019).

Research focusing on defining and measuring the cybersecurity culture is considered to be lacking (Gcaza & van Solms, 2017). A few industry-based papers are suggesting that measuring

cybersecurity culture should be done following the cybersecurity elements (e.g. Tree Solution, 2020), similar to those shown in our conceptual model.

Three different approaches can be employed by an organisation to produce a pre-treatment cybersecurity culture current situation before they implement their selected programmes. One is to measure cybersecurity culture separately from the treatments to be employed. The second is to use the selected metrics of the treatments as the current situation. The third is to conduct both approaches together. All three approaches are employed within organisations that have actively developed cybersecurity culture programmes.

APPROACH 1: DETERMINE A CYBERSECURITY CULTURE CURRENT SITUATION INDEPENDENTLY FROM THE CSC INTERVENTIONS

Using this approach, calculating a current situation measurement or cybersecurity 'score' for the organisation is achieved by conceptualising cybersecurity culture as one or more dimensions to be measured via a data collection process. This cybersecurity score is determined separately from the interventions, hence is not a step included in the step-by-step implementation guide for cybersecurity programmes.

APPROACH 2: DETERMINE A CYBERSECURITY CULTURE CURRENT SITUATION BY UTILISING THE INTERVENTION METRICS

Using this approach, the cybersecurity culture's current situation as part of the step-by-step implementation guide is developed by taking the results of the pre-treatment metrics and using these as the current situation. This approach uses the physical manifestation of cybersecurity-relevant activities of people as the cybersecurity current situation of that organisation. This entails the following steps:

Step 1: Create a list of metrics relevant to the cyber security activities of the organisation.

Step 2: Calculate pre-treatment values of these metrics through whatever data collection methods are most appropriate. These values constitute the current cybersecurity culture situation.

Step 3: Develop and implement the cybersecurity culture interventions, employing the implementation framework/model.

Step 4: Re-measure these metrics by calculating their post-treatment values to determine any changes in the organisational cybersecurity levels.

APPROACH 3: COMBINE APPROACHES 1 AND 2

Given that both of the two previous approaches possess unique benefits, and many of the drawbacks of each approach are addressed by the other, the cybersecurity culture implementation team may choose to employ both approaches 1 and 2. If this third, combined

approach is adopted, the cybersecurity culture team may select to measure the overall cybersecurity culture score (as outlined in approach 1) periodically (e.g., annually, bi-annually, etc.) to provide a higher-level picture of your organisation's cybersecurity culture, while measuring specific behaviours as part of the ongoing cybersecurity culture activities (as outline in approach 2).

CHAPTER 5: RESEARCH METHODOLOGY

RESEARCH PROBLEM

Technologies cannot protect organisations if incorrectly integrated and utilised. Hence, the majority of data breaches within organisations are the result of human actors. Furthermore, while cybersecurity policies are commonplace among organisations, people may view them as guidelines rather than rules (Ponemeon, 2012; ENISA, 2018). It is, unfortunately, happening that many times organisations overlook the human factor security depends upon. Hence, technology is often falsely perceived as the immediate answer to cybersecurity problems. However, cybersecurity is primarily a human factors problem, which remains unaddressed and requires immediate attention (Metalidou et al., 2014; Nobles, 2022).

Since people are often the weakest link in an organisation's cybersecurity chain (Teh et al., 2015; De Maggio et al., 2019), organizations should not only provide sufficient security training and resources to their employees (Chatterjee, 2019) but should also create and maintain a culture of cybersecurity awareness (UNECA, 2014; Norris et al., 2019; Zhan et al., 2021). Against this backdrop, the development of a cybersecurity culture influences a change in mindset, fosters security awareness and risk perception and maintains a close organisational culture, rather than attempting to coerce secure behaviour (ENISA, 2018).

There are, unfortunately, no readily available reports regarding the contemporary state of cybersecurity awareness or cybersecurity culture in TVET colleges in South Africa but it would be fairly safe to presume that cybersecurity awareness and capabilities are still low. Hence, it seems that this study is the first of its kind in South Africa, which will help in understanding how to build a cybersecurity culture in TVET colleges in the country.

THE AIM, OBJECTIVES, AND QUESTIONS

This two-phase research aims to achieve the following aim, objectives, and questions:

THE AIM

The main objective of this study is to create an executable action plan that will help to protect TVET students, teachers, managers, and admin staff from becoming victims of cybercrime. At the same time, cybersecurity-aware and trained people at TVET colleges will be a 'protective layer' for other organisations they digitally interact with - including the insurance sector organisations. This aim also supports the SA government's agenda to educate all South Africans on the safe use of the Internet in an attempt to strengthen the cybersecurity capability of the whole country (National Integrated ICT Policy, 2016; Cybercrime Bill, 2016).

The aim of this action study is based on an informed assumption that TVET students, teachers and managers are not yet properly cybersecurity educated or trained hence their digital devices may remain unprotected. This may even leave the South African Internet

infrastructure vulnerable to attacks, posing a severe cyber threat to National security and eventually affecting communities other than those directly involved (Grobler et al., 2011). For example, increasingly occurring ransomware attacks can cripple the entire ICT infrastructure of an educational institution such as TVET colleges. The examples of such attacks are numerous. For example, it was recently reported that successful ransomware attacks on the education sector grew a staggering 388% in Q3 2020 (Tripwire, 2020).

THE MAIN OBJECTIVE

Following the identified research problem, the main objective of this study is formulated as follows:

To identify and define crucial elements of the Conceptual model for building cybersecurity culture in TVET colleges, and to devise an appropriate Action plan.

SECONDARY OBJECTIVES

1. To identify and define crucial elements of the Conceptual model for building cybersecurity culture at TVET colleges.
2. To explore an effective way of integrating these elements into the form of an executable Action plan.
3. To define a way of effectively executing such an Action plan to increase cybersecurity culture in TVET colleges in South Africa.

THE MAIN RESEARCH QUESTION

Following the established objectives, the main research question is formulated as:

“What are crucial elements of the Conceptual model for building cybersecurity culture in TVET colleges, and what are elements of an appropriate Action plan?”

SECONDARY RESEARCH QUESTIONS

The secondary research questions are formulated as:

1. What are the crucial elements of the Conceptual model for building cybersecurity culture in TVET colleges?
2. How these elements can be effectively integrated to form an executable Action plan?
3. What is the way of effectively building and executing such an Action plan for building a cybersecurity culture in TVET colleges in South Africa?

RESEARCH PHILOSOPHY AND THEORETICAL LENS

RESEARCH PHILOSOPHY OF CYBERSECURITY CULTURE RESEARCH

Two main academic disciplines, namely information technology and industrial psychology (Figure 9), can be used to illustrate what aspects should be considered when conducting cybersecurity culture research (da Vega, 2016).

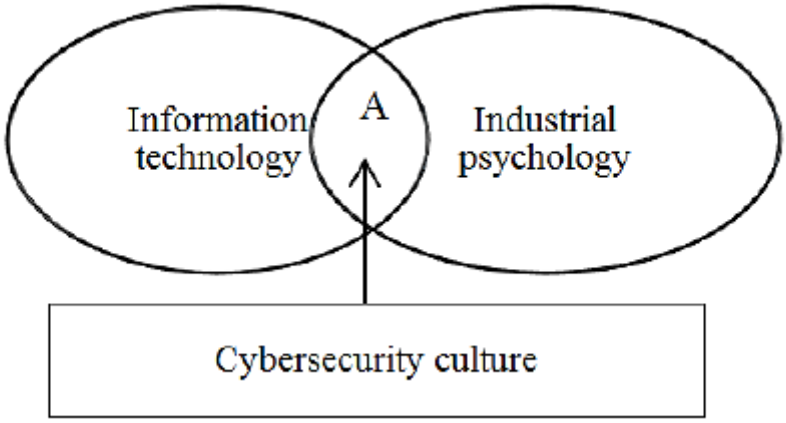

Figure 9: Research fields for cyber security culture (source: da Vega, 2016)

Information technology (IT) **discipline** (through information systems) is concerned with the use of technology, which is a combination of hardware, software, telecommunication systems, and other devices to manage and process information for various purposes (Haag & Cummings, 2013; Von Solms & Van Niekerk, 2013). This, for example, also includes communication, storage, calculations, meeting business objectives, performing tasks, and automation. Da Vega (2016) believes that IT is used as the tool or enabler to process the information or data required to achieve the various purposes of individuals, businesses, and governments.

On the other hand, **Industrial psychology** is the study of human behaviour at work (Howell, 2014) and is used to understand organisational culture and human behaviour. For example, attitudes and perceptions are examined to understand how a cybersecurity culture develops and how it may be assessed. The methods applied in industrial psychology can be used to understand how to integrate cybersecurity and organisational culture to be able to ultimately propose a research approach and methodology for investigating cybersecurity culture (da Vega, 2016).

THEORETICAL LENS OF THIS STUDY

Methodological approaches have referred to the use of theory as analogous to a coat closet in which different items can be housed or a lens through which the literature and data in the study are viewed (Collins & Stockton, 2018). Hence, theoretical frameworks provide a

particular perspective, or lens, through which to examine a topic. There are many different lenses, such as psychological theories, social theories, organisational theories, or economic theories, which may be used to define concepts and explain phenomena.

Reviewing the available literature, this study found the Cybersecurity culture research methodology by da Vega (2016) is appropriate for this research as it is directly related to the topic of this research. Supporting this need, certain scholars have articulated the inextricable presence of theory in the process of obtaining knowledge, describing facts as theory-laden, and noting the influence of a theoretical lens to arrive at observation statements (Flinders & Mills, 1993; Guba & Lincoln, 1994).

CYBERSECURITY CULTURE RESEARCH METHODOLOGY (CSECRM)

Da Vega (2016) suggests that the Cybersecurity culture research methodology is based on the objective to conduct cybersecurity culture research using a measuring instrument that is meaningful and powerful due to its robustness that allows the researcher to draw conclusions and make predictions based on the data obtained. The proposed methodology comprises three key phases (A, B and C) as shown in Figure 10.

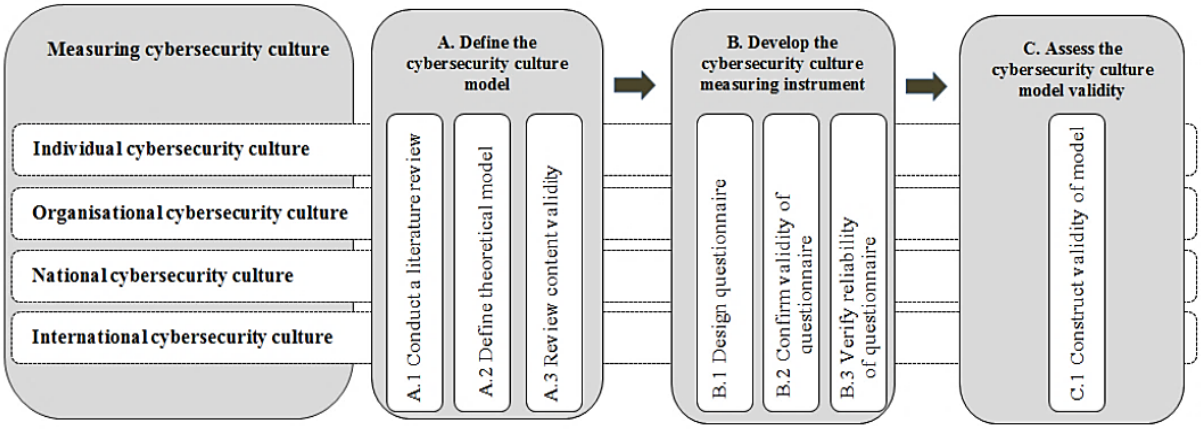

Figure 10: Cybersecurity culture research methodology (CSeCRM) (source: da Vega, 2016)

In phase A, a cybersecurity culture model is defined, followed by the development of the cybersecurity culture measuring instrument in phase B. In phase, C, the validity of the cybersecurity culture model is determined.

Define the cybersecurity culture model

A.1: **Conduct a literature review**

The purpose of the literature review is to gather preliminary information about important issues regarding the cybersecurity culture to be measured. Interviews or group discussions can be used to identify key issues and give the researcher an idea of which questions to ask. This phase of this study is described in the literature review consisting of Chapter 2: A general overview of cybersecurity, and Chapter 3: Cybersecurity culture.

A.2: **Define the theoretical model**

A theoretical or conceptual model is defined to portray the important issues or topics identified in the literature review and related activities. It typically incorporates key concepts and identifies potential relationships and influences between the concepts. A cybersecurity culture model can thus be formulated by depicting the key concepts to be measured. The conceptual model for the development of cybersecurity culture in TVET colleges is given in Chapter 4: Cybersecurity culture implementation conceptual model.

A.3: **Review the content validity of the model**

Content validity evaluates the theoretical perspectives underlying the measuring instrument and how the theory/concept has been used to develop the items that are measured. In the case of the cybersecurity culture questionnaire, content validity can be confirmed by considering the definition of cybersecurity culture and the components of the cybersecurity culture model. This review was done by collecting the verification data using qualitative questionnaires for students, teachers, and managers at the two selected colleges. Additional verification was done by the use of a focus group.

Develop the cybersecurity culture measuring instrument

B.1: **Design the questionnaire**

The constructs identified in the theoretical model are used to design the cybersecurity culture questionnaire statements. The researcher may collect three types of data when doing a survey, namely:

- Opinion variables (i.e. how employees feel about cybersecurity and what they believe is true or false),
- Behaviour variables (i.e. what employees did in the past when using cyberspace, what they do now or what they will do in future), and
- Attribute variables (i.e. characteristics of employees such as their age or grade).

All of the above were used in the study's qualitative survey and the focus group.

B.2: **Confirm the validity of the questionnaire**

Validity is a complicated term, but necessary to consider constructing a powerful research instrument. The concept of validity implies that care must be taken to ensure that the questionnaire assesses what it claims to assess. A valid questionnaire consistently yields reliable and stable results over time. The research team of this study has adhered to these suggestions.

B.3: **Verify the reliability of the questionnaire**

The purpose of this step is to determine the reliability of a questionnaire and the degree to which the items selected "fit into" the intended area (cybersecurity culture) measured. As with the previous point, the research team of this study has adhered to these suggestions.

Assess the cybersecurity culture model validity

C.1: Construct validity of the model

The technique of structural equation modelling (SEM) or similar can be used to determine the construct validity of the cybersecurity culture model. It is suggested by da Vega (2016) that a valid and reliable measuring instrument be used when assessing cybersecurity culture and that phase C be used to complement the validity of the cybersecurity culture model. The construct validity has been assessed, as the previous points, through analysing survey qualitative data and the input from a focus group.

Da Vega (2016) concluded her article by stating that the assessment of the cybersecurity culture level can be incorporated into existing cybersecurity risk management and incident management frameworks to understand the risk from a human perspective in an organisation. This can complement motivations for reduced cyber risk insurance if the culture is at an acceptable level. It can also be used by governments as input to define a cyber strategy to mitigate risks from a user perspective. In this research, the findings of this study can be used by the decision-makers in government and parliament for appropriate policymaking.

RESEARCH DESIGN: PHASE ONE

The interpretive paradigm and inductive logic were deployed in this descriptive and exploratory study.

The Case study research strategy was deployed in the first phase of this study. A Case study methodology, as an in-depth examination of a particular event or individual or a group of individuals (students, teachers, and managers in the researched TVET colleges, in this case), helped in gathering information and reviewing the apposite literature required for developing stage and planning intervention. It also helped in reporting the study results and advising future interventions. This variant of the methodology, which combined the ethos of Action research (planned for the second phase of this study) with the prescriptive mechanism of Case study analysis, was developed and employed by McManners (2015).

Primary data sources in this study were a qualitative questionnaire and key expert focus groups. Secondary data sources include international and national academic and industry reports on cybersecurity and cybersecurity culture.

This research used purposive sampling with a population consisting of 2nd-year students, teachers, and managers of the selected colleges. The sample included 44 qualitative surveys and two focus groups. However, despite the best effort of the research team, supported by the INSETA officials, the data collection was not smooth but despite a smaller-than-expected

sample, the patterns from the collected and analysed data were sufficient to verify the derived conceptual model.

The content analysis was used with the utilisation of the categorical variables (Glen, 2013), given in the section "Variables measured through the analysis of answers to the pertinent questions".

RESEARCH DESIGN: PHASE TWO

Action research is "an approach in which the action researcher and a client collaborate in the diagnosis of the problem and the development of a solution based on the diagnosis (Bryman & Bell, 2011). As the term suggests, action research is an approach that involves both action and research.

The action is usually associated with identifying and exploring an issue, question, dilemma, gap, or puzzle in a particular context and usually involves putting deliberate practical changes or 'interventions' in place to improve, modify, or develop the situation (Fischer, 2001). The research in Action research involves a systematic approach to collecting information, or data, usually using methods commonly associated with qualitative research (Burns, 2009).

In the case of this study, Action research is used for transformative change of the TVET colleges' teachers, students, and managers through the development of cybersecurity culture, done through the simultaneous process of taking action, and doing research.

Theoretical underpinning is based on Torbert's (1981) statement that knowledge is always gained through action and for action. From this starting point, Maintains Torbert, to question the validity of social knowledge is to question, not how to develop a reflective science about action, but how to develop genuinely well-informed action.

In its essence, this study's intervention subscribes to 4-staged Action research, which includes the following:

1. The planning stage.

2. The acting stage.

3. The developing stage.

4. The reflecting stage.

This involves the following steps (adapted from Mertler, 2014):

Step 1: Identifying and limiting the topic, which was done in the first phase of this research. The topic is limited to the development of cybersecurity culture in TVET colleges.

Step 2: Gather relevant information.

Step 3: Review the related literature.

Step 4: Develop a research plan.

Step 5: Implement the plan and collect data.

Step 6: Analysing the data.

Steps 2,3,4,5, and 6 were done in the first phase of this research.

Step 7: Develop an Action Plan, which has been done as the first stage of the study's second phase.

Step 8: Implementing the developed Action plan and monitoring the implementation, which is planned for a new school year.

Step 9: Sharing and communicating the results, will be done after the end of the project.

In collaborative Action research, such as this one, both researchers and participants are engaged together in the provision and implementation of ideas in practice (Brantlinger, et al., 2005 Fletcher & Marchildon, 2014; Schneider, 2012). Participants with their knowledge, therefore, helped the research team to design and collect research evidence, and have contributed to a deeper understanding of the research and its results. Hence, participation in collaborative action research also benefits its participants who can use the research results for advocacy and organisational purposes (Fletcher & Marchildon, 2014).

ETHICAL ISSUES

This research subscribed to the DUT etic code of research. This included obtaining ethical clearance from the University and obtaining consent from the participants of this study. The participants were given a full description of the project through an information sheet and dedicated online sessions. It was also explained to the participants that the collected data will be handled strictly confidential and that all personally identifiable data will be removed. The participants have also been informed that they may, at any time, withdraw from participation in this project. The participation of the staff and students from the selected colleges was approved by their institutions.

CONCEPTUAL LANCES

HUMAN ACTIVITY SYSTEMS

Human Activity Systems (HAS) presume that human beings are rarely predictable in the sense of what they need today will be different from what would they need in the next year. This notion should be taken into consideration while creating preconditions for improving any culture – including cybersecurity culture.

The HAS is classified into three categories: (1) the primary tools, i.e. physical tools or artefacts such as security systems, (2) the secondary tools, i.e. psychological tools such as the language and ideas, and (3) the tertiary tools, i.e. psychological tools such as the culture, which is the main topic of this study.

Stakeholders need to be involved in developing culture as they are part of the system and the environment. HAS addresses the problem that necessitates the development of cybersecurity culture from different dimensions such as (1) meaning engraved within the problem such as the norms, beliefs, and assumptions, (2) social relations such as organisational conflicts, leadership styles, and power, (3) human design factors such as the rules, policies, processes, or environmental factors (Alman, 2013).

THE PROTECTION MOTIVATION THEORY

As already mentioned in this report, Internet users do not feel safe online. They experience threats related to identity theft, malware or viruses, security of financial information, and phishing attacks that may harm their professional reputation and personal lives. Hence, the protection motivation theory (PMT) is used in this study to understand what drives online safety behaviours in the context of the cybersecurity culture.

Based on the theory of reasoned action, PMT interprets how and why individuals decide to undertake protective behaviours, which is motivated by threat and coping appraisal (Tsai et al., 2016). In other words, the PMT deals with how people cope with and make decisions in times of harmful or stressful events in life. These decisions are a way of protecting oneself from perceived threats. The theory attempts to explain and predict what motivates people to change their behaviour.

As Tsai et al (2016) explain, threat appraisals are determined by perceived vulnerability and susceptibility to risks but also by the consequences associated with unsafe behaviours. Coping appraisals are based on coping self-efficacy, response efficacy, and response costs associated with safe or adaptive behaviours of people. In that regard, coping self-efficacy is the belief that individuals can successfully carry out protective behaviours, which is an important presumption in the context of a cybersecurity culture.

Response efficacy is the belief in the effectiveness of the protections, which refers to this study's intent to develop an effective response to cyber threats through the development of a cybersecurity culture. This study also accepts the PMT suggestion that threat appraisals and coping appraisals determine behavioural intentions to adopt cybersecurity culture-related protective measures.

SOCIOLOGICAL PERSPECTIVES

Sociological perspectives or sociological paradigms have been extensively used in research in the forms of (1) the radical humanist, (2) radical structuralist, (3) interpretivists and (4)

functionalist. In the paradigms, there is internal consistency in terms of assumptions about the people and the society under study as well as with the goals being investigated (Burrell & Morgan, 2017).

The four perspectives are mutually exclusive, meaning that two perspectives cannot be utilised at the same time since, by accepting one perspective's assumptions, other perspectives' assumptions are rejected (Pozzebon et al, 2014). This research subscribes to the interpretive paradigm which seeks to understand the social world from the position of subjective experience (Burrel & Morgan, 1979) – in this case of the experience of the participants in this study: TVET students, teachers, and managers.

The interpretive perspective acknowledges that stakeholders are complex so there is no singular solution for different organisations, hence the problems at hand need to be looked at and find the best solution. This perspective supports consensus agreements in the organisation, and this could greatly assist in building culture through communication with various stakeholders.

VARIABLES MEASURED THROUGH THE ANALYSIS OF ANSWERS TO THE PERTINENT QUESTIONS

ATTITUDES

Attitudes also relate to the feelings and beliefs that the TVET colleges teachers and students have toward the security protocols and issues. Attitudes are commonly expressed in terms such as **prefer**, **like**, **dislike**, **hate**, and **love**. Attitudes involve a preference for or against something.

Social psychology has discovered that attitudes are made up of **cognitive**, **affective**, and **behavioural** components (Jhangiani et al, 2014). Here are illustrative examples possibly related to the colleges' students:

- In terms of **affect**: They feel happy when they use modern ICT.
- In terms of **cognition**: They are not fully cognisant regarding possible cyber-attacks and ensuing damages.
- In terms of **behaviour**: Consequently, they do not regularly update their devices.

Affective

Q1: Are you happy with the current cybersecurity state at your institution (e.g. the practice of frequently changing passwords, not using college computers for personal purposes, not using personal devices for teaching or learning purposes)? Please briefly describe.

Cognitive

Q1: How familiar are you with the cybersecurity practice at the college? Please briefly describe.

Q2: Please briefly describe your familiarity with the basic cybersecurity principles or practice.

Behaviour

Q1: Do you adhere to the prescribed cybersecurity practice at the college (e.g. not opening unknown attachments or following the link to an unfamiliar website)? If yes, please briefly describe.

Q2: How often do you visit unfamiliar websites by clicking on the link in an email?

Q3: While receiving an email containing a suspicious link would you:

- Carry on by clicking the link and enjoying the website content.
- Ignore that email and not visit a potentially interesting website.
- Report that email and ignore the suspicious link.

Q4: Somebody recommended to you a website with exciting content but unfamiliar to you. Would you:

- Encourage your peers, relatives or family to visit potentially interesting websites even if are not familiar with the potential damages caused by that action.
- Caution them that website might be dangerous?
- Ignore the recommendation?

COGNITION

Q1: How would you describe your knowledge understanding and awareness of cybersecurity issues?

Q2: What would be a benefit for teachers and students from attending cybersecurity awareness proteomes?

Q3: What would be a benefit for students from a cybersecurity syllabus?

COMMUNICATION

Q1: What is the state of the cybersecurity communication at the college (e.g. quality, frequency, communication channels: email, posters, etc.)?

COMPLIANCE

Compliance refers to knowledge of written cybersecurity policies and the extent that people follow them.

Q1: How familiar are you with the college's cybersecurity policies, rules and procedures?

NORMS

Q1: How familiar are you with the college's cybersecurity norms (e.g. terms of use of the college's ICT equipment)?

RESPONSIBILITIES

Q1: Do you know to whom to report a cyber incident that happened to you? Please describe briefly.

Q2: How do you perceive your role in cybersecurity while at the college?

LAYERS OF CYBERSECURITY CULTURE

Tactic assumptions

Q1: How do you view cybersecurity at the college (e.g. as an integral part of teaching and learning, a separate issue)? Please describe briefly.

Espoused values

Q1: Who is responsible for cybersecurity at the college (e.g. certain departments, management, teachers, everybody)?

Artefacts

Q1: How satisfactory is the college's management involvement in cybersecurity at the institution (e.g. active participation, championing, financing)?

Q2: How training programs and cybersecurity policies are available at the college?

Q3: How familiar are you with the college's cybersecurity policies?

Q4: Briefly describe the usefulness of cybersecurity training programme/s.

FACTOR IMPACTING CYBERSECURITY CULTURE

Q1: How familiar are you with the college's general culture (e.g. acceptable and unacceptable behaviour)?

Q2: How much is currently cybersecurity culture integrated into the college's general culture? Please briefly describe.

The roles to be played by different stakeholders groups

Q1: How well are cybersecurity roles of the stakeholders at the college defined (e.g. senior managers, IT people, human resources, legal department, teachers, students)?

Human factors in cybersecurity culture

Q1: How aware are you of cybersecurity risks for you and the college while using ICT devices (e.g. PCs, tablets, smartphones)?

Q2: How much do others influence your behaviour while using ICT devices at the college or in the online interaction with the college? Please describe briefly.

Q3: How much the environment influences your behaviour while using ICT devices at college or in the online interaction with the college? Please describe briefly.

Q4: In what way general national environment and happenings influence your behaviour related to the use of ICT at college or in the online interaction with the college?

CYBERSECURITY CULTURE STRATEGY

Q1: To what extent are you familiar with the cybersecurity strategy? Please describe briefly.

Q2: How effectively is the college's cybersecurity strategy is implemented?

IMPROVING CYBERSECURITY CULTURE THROUGH EDUCATION

Q1: Is there a syllabus dedicated to cybersecurity or cybersecurity culture? Please describe briefly.

Q2: How often is conducted cybersecurity training or cybersecurity awareness campaigns? Please describe briefly.

FORMS OF DELIVERY CYBERSECURITY CULTURE PROGRAMMES

Q1: How cybersecurity syllabus and awareness campaigns are delivered (e.g. online, offline, combined)? Please describe briefly.

MEASURING CYBERSECURITY CULTURE PROGRAMMES

Q1: How has cybersecurity culture been measured thus far? Please describe briefly.

The analysis of these above questions that were posed to the participants from the two selecting colleges was also used for the verification and validation of the Conceptual implementation model for developing cybersecurity culture at TVET colleges (Figure 8), which is developed by this study.

CHAPTER 6: THE CURRENT STATE OF CYBERSECURITY CULTURE IN THE SELECTED COLLEGES

The Cybersecurity culture implementation conceptual model derived by this study is verified following the conceptual lances, i.e. "Cybersecurity culture research methodology (CSeCRM)" (da Vega, 2016), which is described in the Research methodology chapter. More precisely, this study's Conceptual implementation cybersecurity culture model was verified and validated following Da Vega's suggestions for developing a cybersecurity culture measuring instrument as well as the guidelines for the assessment of the cybersecurity culture model validity.

This process started by developing the qualitative questionnaire according to the identified constructs belonging to the Conceptual implementation model for developing cybersecurity culture at TVET colleges (Figure 8).

These questions are given in the previous chapter and include:

- Opinion variables (i.e. how the participants feel about cybersecurity and what they believe is true or false).
- Behaviour variables (i.e. what the participants did in the past when using cyberspace, what they do now or what they will do in future), and
- Attribute variables (i.e. characteristics of the participants such as their age or grade).

All the above were used in the study's qualitative survey and the focus groups.

The confirmation of the validity of the questionnaire implied that care was taken to ensure that the questionnaire assesses what it claims to assess. Hence, the research team believes that the questionnaires for students, teachers, and managers consistently yielded reliable and stable results.

The verification of the reliability of the questionnaires was done by determining the reliability of a questionnaire and the degree to which the items selected "fit into" the measuring cybersecurity culture in the selected colleges. As with the previous point, the research team of this study has adhered to these suggestions.

The construct validity of this study's conceptual model has been assessed, as the previous points, through analysing survey qualitative data and the input from the focus groups.

FINDINGS: THE CURRENT STATE OF CYBERSECURITY CULTURE IN THE SELECTED COLLEGES ACCORDING TO THE "CONCEPTUAL IMPLEMENTATION MODEL FOR DEVELOPING CYBERSECURITY CULTURE"

As per the explanation in the final section of the previous chapter, the participants were divided into three groups: (1) students, (2) teachers, and (3) teachers and managers. The questions probed the participants' perception of the components belonging to the constructed Conceptual implementation model for developing cybersecurity culture at TVET colleges: (1) Attitudes, (2) Cognition, (3) Communication, (4) Compliance, (5) Norms, (6) Responsibilities, (7) Layers of cybersecurity culture, (8) Factors impacting cybersecurity culture, (9) Cybersecurity culture strategies, (10) Improving cybersecurity culture through education, (11) Forms of delivery cybersecurity programmes, and (12) Measuring cybersecurity programme.

The analysis of the participants' answers is presented here by describing the current state of the major components of the Conceptual model and their elements. It is worth mentioning that there was no difference in answers from the research urban (Elangeni) and rural (Umfolozi) colleges.

THE STATUS QUO OF THE DIMENSIONS OF CYBERSECURITY CULTURE

The status quo of the Attitude component

The Attitude component was measured by three elements: Affective attitude, Cognitive Attitude, and Behaviour.

AFFECTIVE ATTITUDE

The respondents have mainly confirmed that they feel happy about using contemporary ICT. Here are a few examples:

"*It feels good and has a new challenge*".

"*I feel like I gain more experience of being an IT technician while I'm still learning*".

"*As I love modern technology, it makes me feel so happy*".

COGNITIVE ATTITUDE

Regarding their familiarity with the cybersecurity practices at their respective colleges, this research finds that the majority of the students are not fully cognisant regarding possible cyber-attacks and ensuing damages. Many of them replied that they are not much aware of possible cyberattacks:

"*I'm not well aware*".

"*I'm not that aware of cyber but I know that they're targeting and destroying information*".

"*Not that much but I'm aware*".

"*No idea at all*".

BEHAVIOUR

The participants' behaviour was tested by asking questions about the prescribed cybersecurity practices of their institutions, visiting unfamiliar websites, receiving emails containing suspicious links, and behaviour when recommended (by someone else) to visit unfamiliar websites.

Adhering to the institutional prescribed practices was negative to the vast majority of the participants, i.e., they confirmed that they are not adhering to these practices, but some confirmed the importance of the prescribed practices:

"*True because it may be a virus in that link to hack the college*".

The majority of participants negated visiting unfamiliar websites but, despite not knowing what could happen by visiting an unfamiliar website, some participants confirm visiting those websites:

"*Very often…90%...*"

"*More often*".

Some of the participants rely on technology to protect them against unknown attachments:

"*Yes, the college computers don't allow students to open unknown files and attachments*".

Asked about the reporting behaviour, a vast number of the participants replied that they would ignore the suspicious link and then report it:

"*Report that email and ignore the suspicious link*".

"*Ignore that email and do not visit a potentially interesting website*".

Analysing the answers related to this element, it was noticeably found that most respondents simply copied the questions and pasted them as their answers. This indicates that the answers cannot be accepted at the face value and that the actual behaviour in this regard might be different.

Regarding the respondents' behaviour when somebody recommends an unfamiliar website with potentially exciting context, most of them stated that they would either ignore the recommendation or caution people that visiting the particular website can be dangerous. However, some of the respondents stated that they would:

"*Encourage peers, relatives or family to visit potentially interesting websites even if are not familiar with potential damages caused by that action*".

The conclusion about the Attitude component:

The Affective attitude element of Attitude was partially satisfactory as the respondents expressed a positive attitude towards the use of modern ICT. However, the elements of Cognitive attitude and Behaviour showed the need for improvements, which can be done by developing appropriate cybersecurity culture.

The status quo of the cybersecurity Cognition

Asked to describe their cybersecurity knowledge, the surveyed teachers gave a mixed response: from not at all and minimum knowledge to average and good. Only one has confirmed attending a cybersecurity course:

"*Good, I have done the SISCO Courses*".

The student's answers on the topic were also mixed: from no knowledge to some familiarity and rare answers that their cybersecurity knowledge is good:

"*I'm, not aware of any*".

"*I don't have any information about it*".

"*My knowledge of cybersecurity is a bed*".

"*I learned through cisco and acquired skills on how to prevent cyber-attacks and ways to bring safety upon not being a victim of cyber-attacks as an individual also as a company*".

Or even contradictory:

"*I think it's good though I don't know much about it*".

From the very general answers by many of the participants can be concluded that their knowledge of cybersecurity is not sufficient:

"*My opinion is that, is the use of digital devices such as phones, laptops and computers and so on*".

"*Protect your device from theft*".

"*Cybersecurity is a defence or practice of protecting system, programming*".

Or even answers not related to cybersecurity knowledge:

"*I have watched a few movies about cyber intelligence I can say I am a little familiar*".

"*My familiarity with my college is much on education process*".

Asked about the possible benefits of attending a cybersecurity awareness programme, all surveyed teachers agreed that there will be significant benefits of attending such a programme. Here are some verbatim confirmations:

"*It will make us well informed and address any misconceptions that we might have*".

"*To understand the impact of cybersecurity in our daily social life and even at work*".

"*Lecturers and students will be able to use the internet safely and avoid being victims of any form of cybercrimes*".

"*For the lecturers to be well informed about the importance of keeping the confidential data as confidential more especial when it comes to matters which might affect the entire college*".

The conclusion about cybersecurity Cognition:

While the respondents recognised possible benefits from cybersecurity awareness programmes, their cybersecurity knowledge was still inadequate for sound protection while interacting online. Hence, the Cognition component needs improvement.

The status quo of cybersecurity-related Communication

The state of the cybersecurity-related communication was labelled as none or not effective:

"*There is no communication about cybersecurity*".

"*Not effectively conducted - poor quality*".

"*I'm not sure if teaching the intro to cyber security course to students counts as communication*".

The conclusion about cybersecurity Communication:

The responses to the communication questions indicate that this component of the cybersecurity culture Dimension category should be improved.

The status quo of cybersecurity Compliance

As cybersecurity compliance is related to written cybersecurity policies, the question was about the familiarity of these policies and whether people at the surveyed colleges follow them. The answers from students and teachers were unanimously negative – here are some examples:

"*I'm not aware of cybersecurity policies*".

"*There is no policy on cybersecurity*".

"*There are no policies or procedures*".

"*I don't know if there is such a policy*".

Other answers were stating that there are some policies but not about cybersecurity:

"*There is a laptop usage policy which outlines guidelines with regards to the use of that college ICT equipment*".

The conclusion about cybersecurity Compliance:

The answers to the compliance questions indicated that there are no cybersecurity policies, or the respondents were not aware of such documents. This part of the Dimensions of cybersecurity culture needs considerable improvements.

The status quo of cybersecurity Norms

The familiarity with the cybersecurity norms by the respondents was similar to the familiarity with the cybersecurity policies. These are typical answers:

"*I am not familiar*".

"*Not very familiar*".

There were also answers which show that the respondents are not even familiar with the term "cybersecurity norms":

"*The equipment and machines are of high quality*".

The conclusion about the cybersecurity Norms:

As with cybersecurity policies, the respondents were not familiar with cybersecurity norms at their respective colleges. Hence, this part of the Dimensions of cybersecurity culture needs considerable improvements.

The status quo of cybersecurity Responsibilities

The question of reporting cybersecurity also produced mixed answers from surveyed teachers:

"*I do not know, but I assume it should be the management team*".

"*None communicated in a cybersecurity policy I know of but guess I'd report to the campus IT*".

"*Yes - Direct Supervisor and ICT Technician on Campus. Escalated to Assistant Director: IT*".

"*To the college central if I encounter any challenges but I have never seen anyone experience that* ".

The surveyed students mainly replied "No". In two instances the answer was "IT department" but some of them were not aware that the first instance of reporting cybersecurity incidents should be their teachers and IT department:

"*Yes, by reporting to the nearest Police department or report it as a tip*".

"*Departments of homeland security*".

"Well, usually you contact your service provider".

Asked about their role in institutional cybersecurity, teachers and managers gave answers that describe their responsibilities in protecting their data and information but none of their responsibilities within their institution:

"*I need to protect the authentication information assigned to me so as not to expose the college system to attacks, watch out for email-related hacks and contribute to stopping viruses*".

Some respondents stated the need to protect their organisation but not mentioning their particular roles:

"*To make sure that my data and my organizational data are secured*".

"*It should play an important role because my actions could have adverse and very severe effects on the entire College IT system. My actions and behaviour online are very important*".

Some of the respondents stated clearly that they are not familiar with their cybersecurity role within the institution:

"*I know that college data needs to be protected but I do not know my role and to what extent must I play it*".

The conclusion about cybersecurity Responsibilities:

The analysis of the responses regarding the cybersecurity responsibilities within the respective colleges showed that either the responsibilities are not defined, or the respondents are not familiar with their cybersecurity responsibilities within the institution. This part of cybersecurity Dimensions needs significant improvements.

The conclusion of the Dimensions of cybersecurity culture status quo:

Summing up the analysis of the **Attitudes** component, it can be concluded that there is satisfactory Affective behaviour regarding the use of modern ICT by the respondents. However, there is considerable room for improvement in the other two elements of this component:

- Cognitive component, as many respondents are not familiar with the cybersecurity practices at their respective colleges.
- Behaviour component, as many respondents have not convinced the researchers that they would behave appropriately in the above-described cybersecurity situations.

In a nutshell, the Attitude component appeared as important so it must be further developed among the stakeholders at the researched TVET colleges.

While the respondents recognised possible benefits from cybersecurity awareness programmes, their cybersecurity knowledge was still inadequate for sound protection while interacting online. Hence, the **Cognition** component needs further improvement.

The respondents have recognised possible benefits from cybersecurity awareness programmes but their cybersecurity knowledge was still inadequate for sound protection while interacting online. Therefore, the **Cognition** component needs additional development.

The responses to the cybersecurity **Communication** questions indicate that this component of the cybersecurity Dimension category should be enhanced.

The answers to the compliance questions indicated that there are no cybersecurity policies, or the respondents were not aware of such documents. Consequently, the cybersecurity **Compliance** component of the Dimensions of cybersecurity culture needs considerable improvements.

As with cybersecurity policies, related to the Compliance component, the respondents were not familiar with cybersecurity norms at their respective colleges. Hence, the **Norms** component of the Dimensions of cybersecurity culture also needs considerable advancements.

The analysis of the responses regarding the cybersecurity **Responsibilities** within the respective colleges showed that either the responsibilities are not defined, or the respondents are not familiar with their cybersecurity responsibilities within the institution. This part of cybersecurity Dimensions needs significant improvements. In other words, the researched colleges must define students, teachers and managers cybersecurity-related responsibilities.

In a nutshell, all components of the Cybersecurity culture **Dimensions** category need additional enhancement to serve the appropriate development of cybersecurity culture at the two researched TVET colleges.

THE STATUS QUO OF CYBERSECURITY CULTURE LAYERS

The participants' view of cybersecurity at the college (e.g. as an integral part of teaching and learning or separate issue tacit assumptions), which presents the notion of Tacit assumptions,

reflected the majority opinion that it should be an integral part of teaching and learning but this practice is still in its infancy. Here is an example of a typical response:

"*It should be an integral part of teaching and learning because we cannot teach computer-related subjects without it. But currently, it is a separate issue altogether, and is not given emphasis*".

"*To be incorporated in Computer literacy courses*".

Answering the question about the responsibility for cybersecurity at the college, which relates to Espoused values, the majority of the participants pointed out their IT departments. However, some of the participants pointed out that cybersecurity "*Should be everyone from end-users to specific departments responsible for cybersecurity*". This responsibility is, however, yet to be formalised.

A group of questions included the management's involvement in cybersecurity, familiarity with the policies, and availability and usefulness of cybersecurity programmes.

The surveyed students stated that they are not familiar with the cybersecurity policies, which relates to the Artefacts layer of cybersecurity culture:

"*I'm not familiar with cybersecurity*".

"*I don't know if there is such a policy*".

Or gave the answers that indicate their unfamiliarity with the topic:

"*I respect my college policies*".

"*I am familiar as I know that I should be the one who protects the system of my institution*".

Regarding another artefact of cybersecurity culture, i.e. availability of cybersecurity-related programmes, some of the participants replied that there are some programmes:

"*Only the online Cisco Cyber Security training course and no policy in place - to my knowledge*".

"*All NCV level 3 students are taken through a Cybersecurity course to also improve their awareness on issues of being safe online and how to contribute to a good cybersecurity environment*".

Other participants stressed that there are no such programmes:

"*I have no idea*".

"*There are no training programmes, but I would default in believing that there is a policy in place*".

The question about the perceived usefulness of cybersecurity programmes yielded mixed but mainly confirmatory answers:

"*I have no idea*".

"*Learning how to protect themselves in cyberspace*".

"*It will equip the students with the importance of keeping information*".

"*The world is moving towards digitalization therefore students must gain proper information in terms of the advantages and disadvantages of such. They need to be empowered with knowledge so that they can be protected at all times when accessing such services*".

The conclusion regarding cybersecurity culture Layers

The participants confirmed their understanding that cybersecurity should be an integral part of teaching and learning practice to support the development of cybersecurity culture. The analysis of the participants' answers regarding the Espoused values suggests that many of them still do not understand that cybersecurity responsibilities should include all stakeholders at their respective institutions.

Most of the respondents also believe that cybersecurity programmes will be useful for the development of a cybersecurity culture. However, familiarity with the institution's cybersecurity policies is still very low.

Minding the above, it can be concluded that the Layer component of the Conceptual model is only partially satisfactory (i.e. Tacit assumptions) but needs improvement.

THE STATUS QUO OF THE CYBERSECURITY CULTURE FACTORS

The question about familiarity with the institutional general culture yielded very mixed answers:

"*Not at all*".

"*Not much*".

"*Yes, I am very familiar*" – with no further explanation.

"*Unacceptable we don't have enough resources...*".

"*Acceptable because learning new ways improves individual being*".

"*No institution can allow disrespectful behaviour so by that am familiar with what is needed in my institution*".

"*They need learners who follow their protocol*".

The analysis of these and other answers suggests that many respondents do not understand the term organisational culture. Hence, it was expected that the respondents would comprehensively answer the question regarding the integration of cybersecurity culture into the organisational general culture. The responses confirmed that expectation:

"*Not so very sure*".

"*I am not familiar with such*".

"*Needs improvement*".

"*Encourage students to keep private information such as personal bank pin codes*".

The question of how well the cybersecurity roles of the stakeholders at the college are defined yielded answers suggesting that there are not clearly defined cybersecurity roles to be played by various stakeholders:

"*Very poorly defined - not sure of each person's role*".

"*No roles yet*".

"Roles are not defined".

"*I do not know; nothing has been said about cybersecurity*".

"*I am not aware of how roles are defined as per policy*".

"*I think senior managers, IT people, and Human resources*".

"*Senior managers, IT people*".

The role of the human factor in cybersecurity was also poorly understood by the majority of the participants. Asked about the awareness of cybersecurity risks, the participants offered mixed answers, from not aware, and very aware to unrelated answers:

"*I'm not aware*".

"I am very aware".

"*ICT make you use passwords wisely, be smart about your data and protect you against identity theft*".

"*Risks grow more complex every day and are forcing organizations to develop attainable action plans that address and mitigate security risks*".

"*Guidelines for creating and safeguarding passwords*".

The answers to the question of how much others influence their behaviour while using ICT were also diverse from sensible to loosely related, showing a mixed understanding of human factors in cybersecurity culture:

"*They don't influence my behaviour*".

"*They influence me positively because their information and identity will remain protected and safe by using ICT*".

"*Well, they have a huge influence since they get to assist me where needed*".

"*Well aware of almost any and every*".

"*The disturbance can be more difficult*".

"*The study revealed several components that influence the decision of teacher use ICT in the classroom. Use of technological tools for teachers and students*".

"*60% of students tend to do wrong things such as sending an unrelated link to our device and expect us to link on it*".

"*We all have a problem with our college Wi-Fi connection poor sometimes we end up asking each other "how is your network on your computer?*"

The influence of the environment on the participants' behaviour while using ICT was also diverse, but also shows still insufficient understanding of the environmental influence of the secure use of ICT:

"*It doesn't influence me*".

"*Not much because we don't interact much*".

"*Not that much, but they saying I use ICT devices too much*".

"*It influences me a lot*".

"*Makes my mind more clear and function good*".

"*The environment behaviour interferes a lot as sometimes the network can fail due to bad weather conditions*".

"*It fools a proof gadget to use for online interaction which ensures the safety of each individual*".

The responses to the question about the influence of national environmental behaviour while using ICT showed mainly an insufficient understanding of this influence:

"*We are a connected world, and the general environment influences our behaviour and actions online*".

"*Nothing so far*".

"*There is no impact on us - our behaviour is not changed*".

"*Be aware of cybersecurity issues*".

"*It's difficult to say because I am not familiar with cybersecurity*".

"*It should have a big influence - but currently we don't take notice*".

"*The many news of company systems being accessed by unauthorised users resulting in loss of data, funds and even access to whole systems being denied, the methods these unauthorised users access these network systems make me more aware and want to do more (simple as a regular change of password) to contribute to a safe cybersecurity environment*".

The conclusion regarding Factors impacting cybersecurity culture

According to the analysis of the responses, it can be concluded that familiarity with the general culture, which influences cybersecurity culture, is not satisfactory. The fact that many respondents did not understand the concept of general culture confirms this finding.

The cybersecurity roles in the surveyed institutions were not clearly defined so this factor of the cybersecurity culture can be deemed as underdeveloped. The same holds for the understanding of the role of the human factor in cybersecurity. The influence on the respondents' behaviour while using ICT by the internal and external environmental factors is also not clearly understood by the participants in this study.

Minding the above, it can be concluded that, to develop appropriate cybersecurity culture, the researched institutions should focus on improving the factors such as better familiarity with the organisational general culture, the cybersecurity roles, the importance of human factors in cybersecurity as well as the influence of internal and external factors on human behaviour while interacting with modern ICT.

THE STATUS QUO OF THE CYBERSECURITY PRACTICES

The status of current cybersecurity practices was probed through questions regarding management support, cybersecurity policies, involvement and communication, cybersecurity awareness and training, and learning from experience.

As stated in the previous sections, the respondents are mainly unaware of the relevant policies and have also pointed to inadequate communication. Here is an example of the state of cybersecurity culture awareness at the researched institutions:

"*There is no cybersecurity culture. Cybersecurity awareness is needed first*".

The management support was not explicitly confirmed but some discussions with a few managers indicated that the managers' support for cybersecurity initiatives will not be problematic.

Regarding cybersecurity awareness and training, the responses from the teachers were mixed: from very limited to average:

"*My knowledge about cybersecurity is very limited. never be trained in cybersecurity*".

"*Average. I learn new things as I go*".

"*I am aware of it but not with the full information*".

Some of the surveyed managers also confirmed low cybersecurity awareness:

"*No awareness has taken place*".

"*Not that I know of*".

"*Not as much [aware]. Only during training*".

However, the respondents stated the absence of continuous training:

"*There hasn't been any training*".

"*Once only - the Cisco online training*".

"*…not in full swing and few employees have received this training*".

"*I am aware that some lecturers attend trainings on it but not Support Staff*."

From the surveyed students' perspective, it seems that students are obtaining cybersecurity awareness almost exclusively through the newly established curriculum:

"*NCV level 3 students are taken through a Cybersecurity course to also improve their awareness on issues of being safe online and how to contribute to a good cybersecurity environment*" – this was a citation from one of the surveyed teachers.

The surveyed students confirmed the above citation:

"*I'm, not aware of any…*"

"*I don't have any information about it*".

The learning from experience was not mentioned by the participants in this study but, according to other answers, it can be concluded that there was no practice of learning from cybersecurity-related experience.

The conclusion regarding cybersecurity Practices at the researched colleges

According to the participants' responses, it seems that the managers at the researched colleges will be willing to support cybersecurity initiatives. However, lacking not known cybersecurity policies, inadequate cybersecurity awareness and training, as well as the absence of learning from experience practice suggest that these elements of cybersecurity culture need considerable improvements. Also, the analysis of the responses suggests that the stakeholders in this research (students, teachers, and managers) do not currently have the potential to positively contribute to cybersecurity at their institutions.

In a nutshell, the cybersecurity practices at the researched colleges are almost non-existent so these elements should be enhanced if an appropriate cybersecurity culture is to be built at those institutions. Minding the willingness of the surveyed managers to support the development of cybersecurity culture but a low level of development of other elements of cybersecurity culture practice, this category can be considered only partially developed.

STATUS QUO OF THE STRATEGY ISSUES AT THE RESEARCHED INSTITUTIONS

Similarly, with the cybersecurity policies issues, the surveyed teachers and managers confirmed non-familiarity or nonexistence of cybersecurity strategies:

"*Not familiar with our Cyber Security strategy*".

"*Not very familiar*".

"*No clue*".

"*No strategy*".

"*Not sure if the college has a strategy*".

"*Anything to do with college strategy involves a senior management team, I am not familiar with any cybersecurity strategy*".

"*It has not been implemented, if it had maybe it was on the IT and TVETMIS department who deals with college and students' data*".

"*The college just started with cyber-security and most employees are yet to know this from employers' point of view*".

The other questions regarding strategy such as the cybersecurity-related environmental assessment or strategy control were irrelevant having in mind the respondents' total unfamiliarity with the institutional cybersecurity strategies.

The conclusion regarding Strategy issues at the researched institutions

There is not much to be concluded regarding cybersecurity strategy issues but to recommend to the management of the surveyed institutions to critically pay attention to the development

and implementation of appropriate cybersecurity strategies as they are a vital element of a sound cybersecurity culture.

THE STATUS QUO OF THE EDUCATION AND TRAINING CURRICULUM

The introductory discussion about the participation of the selected colleges in this study revealed the fact that there was not any specific subject on cybersecurity culture. Furthermore, there were not any other activities regarding the development of cybersecurity culture.

"*Not specifically in my program*".

However, the inspection of the current curriculum confirmed that there are some cybersecurity courses, which promote and offer some cybersecurity knowledge:

"*It has just been introduced in the year 2022 for level 3 lecturers and students*".

"*DHET introduced cybersecurity subject in NC(V) L3*".

One of these courses is "Introduction to Cybersecurity", which covers the following:

- Learning the basics of being safe online;
- Learning about different types of malware and attacks, how organisations are protecting themselves against these attacks; and
- Exploring career options in cybersecurity.

The other course is "Computer practice for N4, N5, and N6 levels", which includes computer practice, the study of the integrated components of a computer system (hardware and software), practical techniques for efficient use, and application to solve everyday problems. This course includes the subject "Digital citizenship", which is connected to cybersecurity culture as it includes topics such are:

- Providing an overview and understanding of how ICTs impact modern-day living;
- Being aware of computer-related threats; and
- Using ICTs responsibly.

These courses are introduced at the beginning of 2022 and were regarded by the research team as sufficient for starting the introduction of cybersecurity culture at the selected (and other) TVET colleges in South Africa. However, there was noted a warning for one of participating teachers:

"…a big weakness to our systems is [that the students are] taken through the cybersecurity course when they are at level 3. So, then they begin to understand their role in protecting college and their own devices against cyber criminals".

Although the above-described curriculum in the current use can contribute to the development of cybersecurity culture, according to the pertinent literature, there should be more pertinent topics such are Information culture and ethics, Information and psychological security, psycho-physical effects on the individual and society, information weapons, Legal issues of information society development or the IT crime.

Furthermore, the participants in this study confirmed that cybersecurity awareness is still low and that there were no organised cybersecurity awareness campaigns. This is described in the previous section of this chapter.

The conclusion regarding cybersecurity culture Education and training curriculum

This research has shown that there are some elements of cybersecurity culture in the existing cybersecurity-related curriculum. However, that was not sufficient to build a sound cybersecurity culture at the researched institutions:

The discussion with some teachers at the researched colleges showed that there are ways to introduce cybersecurity culture-related courses or subjects. One of the ways is to introduce particular cybersecurity culture courses, which will require a systemic education intervention – maybe even including such a course at the primary and secondary levels. Having in mind the fact that dealing with modern technology occupies a considerable time of people's work and leisure time – and that that interaction should be protected - this suggestion seems reasonable.

Another way is to introduce particular cybersecurity culture subjects within the existing cybersecurity curriculum. This can be official or unofficial, the latter would be up to the teachers' competencies and willingness.

In a nutshell, the cybersecurity culture curriculum in TVET colleges is currently nonexistent but some subjects feature some cybersecurity culture elements. Hence, future relevant interventions should include courses or subjects that will directly contribute to the development of sound cybersecurity culture.

The status quo of the Forms of delivery cybersecurity culture

Since this research found out that there were no particular courses or subjects on cybersecurity culture as well as that there were no particular cybersecurity culture awareness campaigns, there was discussion on forms used for delivering this kind of culture. However, asked about their opinion of the ways that should be used for delivering cybersecurity culture, the majority of respondents pointed out the combined online and offline approach, which will include cybersecurity courses and subjects as well as cybersecurity awareness campaigns.

The status quo of Measuring cybersecurity culture

Since there were no specific programmes for the development of cybersecurity culture, there was no developed instrument for measuring cybersecurity culture at the researched TVET colleges:

"*Cyber Security has not been measured thus far - to my knowledge*".

"*I have no idea*".

Hence, it can be concluded that the measuring component of cybersecurity culture is lacking and should be introduced in further plans for delivering cybersecurity culture in TVET colleges.

THE FINDINGS CONCLUSIONS

The analysis of the response by students, teachers, and managers to the qualitative survey shows that the cybersecurity culture at the researched institutions is in its embryonic state, as shown in Table 4.

Table 4: The state of the Categories and elements of cybersecurity culture at the researched TVET colleges (source: Authors)

Category	Elements	Developed	Partially developed	Underdeveloped
Dimensions	Attitudes		x	
	Cognition			x
	Communication			x
	Compliance			x
	Norms			x
	Responsibilities			x
Layers	Tacit assumptions		x	
	Espoused values			x
	Artefacts			x
Factors	Organisational			x
	Human			x
	External			x
	Social environment			x
Practices	Management support		x	
	Cybersecurity policy			x
	Cybersecurity awareness and training			x
	Involvement and communication			x

	Learning from experience			x
Implementation strategy & guidelines	Strategy direction			x
	Environmental assessment			x
	Strategy formulation			x
	Strategy implementation			x
	Strategy control			x
	Specific implementation steps			x
Education & training curriculum	Curriculum cybersecurity culture topics			x
Forms of delivery	Online			x
	Offline			x
	Hybrid			x
Measuring (M&E)	Determine cybersecurity culture independently from the interventions			x
	Determine cybersecurity culture by using the intervention's metrics			x
	Combinations of the previous two methods			x

As stated earlier and is visible in Table 4, almost all categories of cybersecurity culture are underdeveloped, except some elements belonging to three categories:

- The Affective attitude element of Attitude was partially satisfactory as the respondents expressed a positive attitude towards the use of modern ICT. However, the elements of Cognitive attitude and Behaviour showed the need for improvements, which can be done by developing appropriate cybersecurity culture.
- Most of the respondents believed that cybersecurity programmes will be useful for the development of cybersecurity culture (i.e. Tacit assumptions). However, familiarity with the institution's cybersecurity policies is still very low. Minding the

above, it can be concluded that the Layer component of the Conceptual model is only partially satisfactory and needs improvement.

- The cybersecurity Practices at the researched colleges are almost non-existent so these elements should be enhanced if an appropriate cybersecurity culture is to be built at those institutions. Minding the willingness of the surveyed managers to support the development of cybersecurity culture but a low level of development of other elements of cybersecurity culture practice, this category can be considered only partially developed.

These findings confirm a need for appropriate intervention for the further development of cybersecurity culture, i.e. the findings confirmed a need for an Action plan aimed at the development of cybersecurity culture in TVET colleges.

VERIFYING EMPIRICAL FINDINGS: THE FOCUS GROUPS INPUT

The results of the analysis of the data collected, shown in the previous sections, were also presented to two focus groups from the two researched TVET colleges: one focus group consisted of five participants and another one of eight participants. The focus groups consisted of 11 teachers and two managers. The purpose of these focus group sessions was to verify the findings coming from the analysis of the qualitative surveys. The focus groups unanimously agreed with the presented findings:

THE STATUS QUO OF THE DIMENSIONS OF CYBERSECURITY CULTURE

Both focus groups agreed that the Affective behaviour regarding the use of modern ICT by the respondents was satisfactory. They also agreed that there is considerable room for improvement in the other two elements of this component: cognitive and behaviour. The agreement is that the Attitude component is important so it must be further developed among the stakeholders at the researched TVET colleges.

The focus groups further agreed that there are possible benefits from cybersecurity awareness programmes, but the knowledge of the stakeholders in the researched college was still inadequate for sound cybersecurity protection. Hence, the Cognition component needs further improvement.

The responses by the focus groups to the cybersecurity Communication status indicate that this component of the cybersecurity Dimension category should be enhanced. The same response was to the finding regarding cybersecurity Compliance – this component of the Dimensions of cybersecurity culture needs considerable improvements.

As with cybersecurity policies, related to the Compliance component, the focus groups confirmed that many of their colleagues are not familiar with cybersecurity norms at their respective colleges. Hence, the Norms component of the Dimensions of cybersecurity culture also needs considerable advancements.

The analysis of the responses regarding the cybersecurity Responsibilities showed that either the responsibilities are not defined, or the respondents are not familiar with their cybersecurity responsibilities within the institution. This part of cybersecurity Dimensions needs significant improvements.

Summarised, the focus groups agreed that all components of the Cybersecurity culture Dimensions category need additional enhancement to serve the appropriate development of cybersecurity culture at the two researched TVET colleges.

THE STATUS QUO OF CYBERSECURITY CULTURE LAYERS

The focus groups confirmed their understanding that cybersecurity should be an integral part of teaching and learning practice to support the development of cybersecurity culture. The focus groups agree that the Espoused values are still not sufficiently understood, i.e. they agree that their colleagues are still certain that cybersecurity responsibilities should include all stakeholders at their respective institutions.

The focus groups further concluded that cybersecurity programmes will be useful for the development of a cybersecurity culture. However, familiarity with the institution's cybersecurity policies is still very low. In summary, it can be concluded that the Layer component of the Conceptual model is only partially satisfactory (i.e. Tacit assumptions) but needs improvement.

THE STATUS QUO OF THE CYBERSECURITY CULTURE FACTORS

According to the focus groups, the familiarity of stakeholders in the researched institutions with the general culture, which influences cybersecurity culture, is not satisfactory. They agree that many stakeholders in this research still do not understand the concept of general culture. Furthermore, the focus groups' participants confirmed that cybersecurity roles in the surveyed institutions were not clearly defined so this factor of the cybersecurity culture can be deemed as underdeveloped. The same holds for the understanding of the role of the human factor in cybersecurity. The focus groups further agreed that the influence on the respondents' behaviour while using ICT by the internal and external environmental factors is also not clearly understood by the stakeholders in this study.

In conclusion, the members of the focus groups agreed that the development of appropriate cybersecurity culture significantly depends on improving the factors such as better familiarity with the organisational general culture, the cybersecurity roles, the importance of human factors in cybersecurity as well as the influence of internal and external factors on human behaviour while interacting with modern ICT.

THE STATUS QUO OF THE CYBERSECURITY PRACTICES

The focus group confirmed that the managers at the researched colleges will be willing to support cybersecurity initiatives. However, lacking not known cybersecurity policies,

inadequate cybersecurity awareness and training, as well as the absence of learning from experience practice suggest that these elements of cybersecurity culture need considerable improvements. Also, they agreed that the stakeholders in this research (students, teachers, and managers) cannot currently positively contribute to cybersecurity at their institutions.

In summary, the focus groups agreed that cybersecurity practices at the researched colleges are almost non-existent so these elements should be enhanced if an appropriate cybersecurity culture is to be built at those institutions. Minding the willingness of the surveyed managers to support the development of cybersecurity culture but the low level of development of other elements of cybersecurity culture practice, the focus groups suggest that this category can be considered only partially developed.

STATUS QUO OF THE STRATEGY ISSUES AT THE RESEARCHED INSTITUTIONS

Since there are currently no official cybersecurity strategies, the focus groups agreed that there is not much to be concluded regarding cybersecurity strategy issues but to recommend to the management of the researched institutions to critically pay attention to the development and implementation of appropriate cybersecurity strategies as they are a vital element of a sound cybersecurity culture.

THE STATUS QUO OF THE EDUCATION AND TRAINING CURRICULUM

The focus groups agreed that there are some elements of cybersecurity culture in the existing cybersecurity-related curriculum. However, that was not sufficient to build a sound cybersecurity culture at the researched institutions. However, the focus groups agreed that there are ways to introduce cybersecurity culture-related courses or subjects. One of the ways is to introduce cybersecurity culture courses, which will require a systemic education intervention. Another way is to introduce cybersecurity culture subjects within the existing cybersecurity curriculum. The focus groups agreed that this can be official or unofficial, the latter would be up to the teachers' competencies and willingness.

In a summary, the focus group members agreed that the cybersecurity culture curriculum in TVET colleges is currently nonexistent but some subjects feature some cybersecurity culture elements. Hence the suggestion that future interventions in this space should include courses or subjects that will directly contribute to the development of sound cybersecurity culture.

THE STATUS QUO OF THE FORMS OF DELIVERY CYBERSECURITY CULTURE

Since this research found out that there were no courses or subjects on cybersecurity culture as well as that there were no particular cybersecurity culture awareness campaigns, the forms used for delivering this kind of culture were not much discussed by the focus groups. However, they agreed that the combined online and offline approach, which will include cybersecurity courses and subjects as well as cybersecurity awareness campaigns, will be appropriate.

THE STATUS QUO OF MEASURING CYBERSECURITY CULTURE

Since there were no specific programmes for the development of cybersecurity culture, there was no developed instrument for measuring cybersecurity culture at the researched TVET colleges. However, the members of the focus groups agreed that measuring the level of cybersecurity culture is important. However, the focus groups concluded that the measuring component of cybersecurity culture is lacking and should be introduced in the further plans for delivering cybersecurity culture in TVET colleges.

THE FOCUS GROUPS FINDINGS AND CONCLUSION

As stated in the earlier sections, (e.g. Table 4) the focus groups agreed that almost all categories of the cybersecurity culture model, developed by this study, are underdeveloped, except some elements belonging to three categories: the Affective attitude element of Attitude, Tacit assumptions and the cybersecurity Practices. Generally, the focus groups agreed that there is a need for appropriate intervention for the further development of cybersecurity culture.

CHAPTER 7: PREPARATION FOR THE INTERVENTION - ELEMENTS OF THE ACTION PLAN

THE INTERVENTION DESIGN

The cybersecurity culture intervention should be applied in the five lifecycle phases: design, build, deploy, operate, and decommission (NIST, 2016). In this study, it is envisaged that the phases will be executed as follows:

DESIGN

This phase includes the design of all interventions, including the timeframe and the variables to be monitored and measured. This phase also includes an agreement with the participating institutions on whether to embrace a **streamlined** or **comprehensive** intervention.

BUILD

This phase includes building or buying the equipment needed for implementing the intervention. This may include additional hardware or software needed for delivering the selected curriculum and communicating appropriate messages. This will also include the equipment for the cybersecurity awareness campaigns (e.g. posters, T-shirts, fliers, etc.)

DEPLOY

When the preceding phases are complete, implementation of the planned programme can start. In this phase, it is important to take a state of the cybersecurity culture at the beginning of the intervention. This phase should last one year or, at least, one semester at the selected colleges.

OPERATE

This includes the delivery of the curriculum and awareness campaign for a streamlined intervention and the inclusion of the cybersecurity risk assessment and the development of appropriate strategies. and policies for the comprehensive development of cybersecurity culture. The curriculum and awareness campaigns can be delivered online, offline or by mixing these two methods.

DECOMMISSION PROGRAMME

After the prescribed period, the programme should be discontinued. However, it can be done only after the new state of the cybersecurity culture is measured and the lessons learned are recorded.

IMPLEMENTATION METHODOLOGICAL ISSUES RELATED TO THE IMPLEMENTATION PLAN

Using the wrong method can hinder the transfer of knowledge and lead to unnecessary expenses and frustrated, purely trained candidates. The best practice suggests the use of short, task-oriented modules the learners need or "just-in-time" training (Trepper, 2006).

According to the absence of evidence of teaching cybersecurity culture at TVET colleges in South Africa, the proposed intervention is not only just-in-time but long overdue. Being a pioneering intervention, this study has applied mainly attributes of cybersecurity awareness and education through the cybersecurity culture curriculum, which is the bases of the streamlined approach. These attributes involved teaching teachers and students what cybersecurity culture is and what they should do in certain circumstances (based on NIST SP 800-12).

In other words, the awareness component seeks to teach teachers and students *what* cybersecurity is and *what* they should do in some situations. The objective is for the teachers and students to recognise threats and formulate a simple response- as a perpetual attitude and behaviour.

On the other hand, the education element seeks to educate students and teachers as to *why* the institutions should prepare to react in a certain way to possible cyber breaches. This is for the teachers and students crucial to understand how to engage in active cybersecurity defence.

All the above should, consequently, contribute to the development of cybersecurity culture through the **education** and **training** component of the Conceptual implementation model for cybersecurity culture at TVET colleges.

The awareness and education category of our model influences crucial elements of cybersecurity culture such as *attitudes*, *cognition*, *norms,* and *responsibilities*. It also influences layers of cybersecurity culture such as *espoused values*.

Cybersecurity awareness, training and education also contribute to the cybersecurity practices element of the proposed cybersecurity culture model in TVET colleges, enabling *learning through experience*.

BASIC ACTIVITIES FOR A STREAMLINED IMPLEMENTATION APPROACH

Regarding the capacitating stakeholders at the researched institutions, the implementation plan should consider the following:

1. Capacitating IT teachers by organising two to four cybersecurity culture-related seminars per year.
2. Capacitating other teachers and managers by organising four awareness campaigns per annum.

3. Capacitating students through syllabus/curriculum and also organising four awareness campaigns per year.

In addition in 2022 were introduced two new cybersecurity-related subjects “Introduction to Cybersecurity” and “Computer practice”, we suggest the inclusion of some of the following topics related to cybersecurity culture (Malyuk & Milosavskaya, 2016):

- Information culture and ethics (e.g. Netiquette).
- Information and psychological security, psycho-physical effects on the individual and society.
- The Internet and freedom of speech.
- Social challenges of the Information society.
- Legal issues of Information society development.
- Cybersecurity Protection laws and regulations.
- IT crime, cyberterrorism, and cyber warfare.

The curriculum can be, depending on available resources and circumstances, delivered online, offline or combined.

PREPARATION FOR THE AWARENESS COMPONENT OF THE PROGRAMME

The cybersecurity awareness programme should be designed to keep cybersecurity at the forefront of the intended audience's minds daily as it serves to instil a sense of **purpose** and **responsibility**. In that regard, the proposed intervention will focus on the following (based o NSIT SP 800-12):

- Focus on people as both parts of the problem and as part of the solution.
- Refrain from using technical jargon but use the language that the attendees understand.
- Use every available venue to access the entire intended audience.
- At the session, define at least one key learning objective, state it clearly, and provide sufficient detail and coverage to reinforce the learning of it.
- Refrain from “preaching” to the audience, i.e. keep things light.
- Do not overload the audience with a great volume of information.
- Help the attendees to understand their cybersecurity role and how a breach can influence the security of the whole college.
- Take advantage of in-house communications media to deliver messages.
- Make the awareness programme formal (e.g. plan and document all actions).
- Provide good information early, rather than perfect information late.

Cybersecurity awareness programme for TVET colleges is also incorporated into basic security training through an already existing IT curriculum which we suggest be modified in agreement

with the selected colleges' relevant teachers. The items included in the awareness programme consist of:

- Videos.
- Posters and banners.
- Computer-based training.
- Newsletters.
- Trinkets (e.g. pens, pencils, T-shirts), if available.
- Brochures and flyers.
- Bulletin boards.

Other relevant items will also be considered as the implementation programmes continue.

The categorical variables that should be measured in the streamlined implementation approach

Following this study's Conceptual implementation model for cybersecurity culture at TVET colleges, the following categorical variables (Glen, 2013) are selected to be probed during and post-intervention period:

1. Attitudes (Affective, Cognitive, Behaviour)
2. Cognition
3. Communication
4. Compliance
5. Norms
6. Responsibilities
7. Layers of cybersecurity culture (tacit assumptions, Espoused values, Artefacts)
8. Factors impacting cybersecurity culture (the roles of different stakeholders groups, Human factors in cybersecurity culture)
9. Cybersecurity culture through education (curriculum impact)
10. Forms of delivery cybersecurity culture programmes
11. Formative and summative evaluation of the development of cybersecurity culture.

The detailed plan will be developed with the participation of the researched TVET colleges and INSETA.

THE COMPREHENSIVE DEVELOPMENT OF CYBERSECURITY CULTURE IN TEVT COLLEGES

STRATEGIC CONSIDERATIONS

As building a strong cybersecurity culture in TVET colleges is crucial for protecting sensitive information, intellectual property, and other valuable assets from cyber threats. The

following is a comprehensive strategic plan to help institutions develop and maintain a robust cybersecurity culture:

1. **Define the objective**: Clearly define the objective of building a cybersecurity culture in the college. This will help to guide the development and implementation of the strategy.
2. **Engage stakeholders**: Engage all stakeholders, including students, faculty, staff, and administration, in the development and implementation of the cybersecurity culture. Ensure that everyone understands the importance of cybersecurity and their role in protecting the institution's assets.
3. **Assess the current state**: Assess the current state of cybersecurity culture within the college to identify areas for improvement. This can be done through surveys, focus groups, or other methods of gathering feedback.
4. **Develop a written policy**: Develop a written policy that outlines the cybersecurity expectations and responsibilities of students, faculty, and staff. This policy should be communicated regularly to all members of the college community and acknowledged by all employees.
5. **Offer cybersecurity training**: Regular training on cybersecurity topics, including best practices for data protection, safe internet use, and password management, should be offered to all employees. Training can be in the form of workshops, online modules, or other learning opportunities.
6. **Promote cyber-awareness**: Regular communication should be sent to all employees on the latest cyber threats and how to stay safe online. This can include email notifications, posters, and other forms of communication.
7. **Implement technical controls**: Technical controls such as firewalls, intrusion detection systems, and antivirus software should be deployed and updated regularly to protect against cyber threats. All employees should be trained on how to use these tools effectively.
8. **Encourage reporting of incidents**: Employees should be encouraged to report any suspicious activity or cybersecurity incidents immediately. A reporting mechanism should be in place, and the response should be prompt, thorough, and professional.
9. **Regular security audits**: Regular security audits should be conducted to ensure that the college's cybersecurity posture is strong and that all employees are following best practices. The results of these audits should be used to continuously improve the college's cybersecurity posture.
10. **Incorporate cybersecurity into curricula**: Cybersecurity should be incorporated into the curricula of relevant courses to ensure that students are equipped with the knowledge and skills they need to stay safe online and to protect their future employers' assets.

11. **Foster a culture of responsibility**: Encourage all members of the college community to take responsibility for their actions and for protecting the institution's assets. This can be done through regular communication and reinforcement of the importance of cybersecurity.
12. **Continuously evaluate and improve**: Regularly evaluate the effectiveness of the cybersecurity culture and make necessary improvements to ensure its continued strength.

By following this strategy plan, TVET colleges can develop a comprehensive approach to building a strong cybersecurity culture, which will protect valuable assets, promote safe and responsible behaviour, and support the success of teachers, students, managers, and employees.

GENERAL GUIDELINES FOR AN ACTION PLAN FOR BUILDING CYBERSECURITY CULTURE IN TVET COLLEGES

The following are general guidelines for a comprehensive action plan to help institutions develop and maintain a robust cybersecurity culture:

1. **Establish a cybersecurity team**: Form a team of individuals responsible for overseeing the development and implementation of the cybersecurity culture. This team should include representatives from various departments, such as IT, academics, and administration.
2. **Develop and communicate a cybersecurity policy**: The first step is to create a written policy that outlines the cybersecurity expectations and responsibilities of students, faculty, and staff. This policy should be communicated regularly to all members of the college community, and all employees should be required to sign and acknowledge it.
3. **Offer cybersecurity training**: Regular training on cybersecurity topics, including best practices for data protection, safe internet use, and password management, should be offered to all employees. Training can be in the form of workshops, online modules, or other learning opportunities.
4. **Promote cyber-awareness**: To promote a culture of cybersecurity, regular communication should be sent to all employees on the latest cyber threats and how to stay safe online. This can include email notifications, posters, and other forms of communication.
5. **Implement technical controls**: Technical controls such as firewalls, intrusion detection systems, and antivirus software should be deployed and updated regularly to protect against cyber threats. All employees should be trained on how to use these tools effectively.
6. **Encourage reporting of incidents**: Employees should be encouraged to report any suspicious activity or cybersecurity incidents immediately. A reporting mechanism

should be in place, and the response should be prompt, thorough, and professional.

7. **Regular security audits**: Regular security audits should be conducted to ensure that the college's cybersecurity posture is strong and that all employees are following best practices. The results of these audits should be used to continuously improve the college's cybersecurity posture.
8. **Incorporate cybersecurity into curricula**: Finally, cybersecurity should be incorporated into the curricula of relevant courses to ensure that students are equipped with the knowledge and skills they need to stay safe online and to protect their future employers' assets.
9. **Foster a culture of responsibility**: Encourage all members of the college community to take responsibility for their actions and for protecting the institution's assets. This can be done through regular communication and reinforcement of the importance of cybersecurity.
10. **Continuously evaluate and improve**: Regularly evaluate the effectiveness of the cybersecurity culture and make necessary improvements to ensure its continued strength.

By following this action plan, TVET colleges can develop a comprehensive approach to building a strong cybersecurity culture.

ESTABLISHING A CYBERSECURITY CULTURE PROGRAMME

The steps that are given in NIST (2017) can be used for the implementation of the Conceptual model developed by this study to create a new cybersecurity culture program or even, later, to improve an existing program. These steps should be repeated as necessary to continuously improve cybersecurity (NIST, 2017). The steps that are recommended to be used in this intervention are as follows:

Step 1: **Prioritisation and Scope**: With this step, the institution makes strategic decisions regarding cybersecurity culture implementations and determines the scope of the intervention. The scope of this kind of programme is much broader than the streamlined implementation described earlier.

Step 2: **Orientation**: Once the scope of the cybersecurity culture programme has been determined, the intervention implementer identifies related systems and assets, regulatory requirements, and overall intervention approach.

Step 3: **Creation of a current cybersecurity profile**: This will be done by measuring current cybersecurity culture variables as outlined in the Conceptual implementation model for cybersecurity culture at TVET colleges, developed by this study.

Step 4: **Creation of a target cybersecurity profile**: This will be done regarding the institutional plans and available resources (e.g. technical, organisational, human resources).

Step 6: **Determining, analysing, and prioritising gaps**: The intervention implementer compares the current profile and the target profile to determine gaps. Next, it creates a prioritised action plan to address those gaps to achieve the outcomes in the target profile. The implementer then determines the resources necessary to address the gaps. Using profiles in this manner enables the implementer to make informed decisions about cybersecurity culture activities and enables the institution under the intervention to perform cost-effective, targeted improvements.

Step 7: **Implementing the action plan**: The implementer determines which actions to take concerning the gaps, if any, identified in the previous step. It then monitors its current cybersecurity culture practices against the target profile.

The Security System Development Life Cycle (SecSDLC) is used for the creation of a comprehensive cybersecurity posture (Whitman & Mattord, 2017), including cybersecurity culture. For that purpose, a system project may be initiated in response to specific conditions. These conditions can be *event-driven* (inside or outside the organisation) or *plan-driven* as a result of a carefully developed planned strategy. In the case of this study, the latter is applicable and refers to the development of cybersecurity culture in TVET colleges.

The preparation for the intervention, according to SecSDLC, starts with a directive from upper management, specifying the process, outcomes, and goals of the project. This also includes a feasibility assessment of the intervention, i.e. the determination of the required resources.

Translated into this project, obtaining agreement and full support from the management of the two selected TVET colleges is the prerequisite. It is also necessary for the management and teachers to agree to the cybersecurity culture transformation, by attending to the categories of the Conceptual implementation model for cybersecurity culture at TVET colleges, and constant feedback as necessary support during a period of change (Winkler & Manke et al., 2015).

RESOURCES NEEDED FOR BUILDING CYBERSECURITY CULTURE IN TVET COLLEGES

To build a robust cybersecurity culture in TVET colleges, a variety of resources are needed. Some of the key resources include:

1. **Financial resources**: Implementing technical controls, providing training, and conducting regular security audits all require financial resources. The college will need to allocate a budget for these activities.
2. **Cybersecurity expertise**: Cybersecurity experts, such as IT professionals, can provide valuable support and guidance in the development and implementation of the cybersecurity culture.

3. **Technology**: The college will need to invest in technology, such as firewalls, intrusion detection systems, and antivirus software, to protect against cyber threats.
4. **Training materials**: The college will need to develop and provide training materials for employees on best practices for data protection, safe internet use, and password management.
5. **Communication tools**: The college will need to utilize communication tools, such as email, posters, and workshops, to promote cyber-awareness and to regularly communicate with employees about the latest cyber threats.
6. **Incident response plan**: The college will need to develop and implement an incident response plan to ensure that all employees know what to do in the event of a cybersecurity incident.
7. **Support from leadership**: The college's leadership must support the development and implementation of the cybersecurity culture, as well as provide the necessary resources to ensure its success.

By investing in these resources, TVET colleges can build a strong cybersecurity culture that will protect sensitive information, intellectual property, and other valuable assets from cyber threats.

ROLES IN BUILDING CYBERSECURITY CULTURE IN TVET COLLEGES

Building a strong cybersecurity culture in TVET colleges requires the involvement and cooperation of many different individuals and groups. The following are some of the key roles in this process:

- **College leadership**: College leadership must be committed to building a strong cybersecurity culture and must provide the necessary resources and support to ensure its success.
- **IT department**: The IT department is responsible for implementing technical controls, such as firewalls, intrusion detection systems, and antivirus software, to protect against cyber threats.
- **Cybersecurity expert**: A cybersecurity expert, such as a consultant or an IT professional with expertise in cybersecurity, can provide valuable support and guidance in the development and implementation of the cybersecurity culture.
- **Human resources**: Human resources can play a critical role in promoting the importance of cybersecurity and ensuring that all employees receive regular training on cybersecurity topics.
- **Employees and students**: All people, including students, faculty, and staff, have a responsibility to protect the college's assets and to follow best practices for data protection, safe internet use, and password management.

- **Curriculum developers**: Curriculum developers can play a critical role in incorporating cybersecurity into relevant courses, ensuring that students are equipped with the knowledge and skills they need to stay safe online and protect their future employers' assets.

By working together, these individuals and groups can build a strong cybersecurity culture that will protect sensitive information, intellectual property, and other valuable assets from cyber threats.

THE OPTIMAL TIME FOR BUILDING CYBERSECURITY CULTURE IN TVET COLLEGES

There is no one "optimal" time for building a cybersecurity culture in TVET colleges, as the timing will depend on several factors, including the level of current cyber threats, the college's current security posture, and the availability of resources.

However, it is generally recommended to start building a cybersecurity culture as soon as possible, as the threat landscape is constantly evolving and new risks are emerging all the time. The earlier a college starts building its cybersecurity culture, the better equipped it will be to protect itself against future cyber threats.

Additionally, building a cybersecurity culture is a continuous process and requires ongoing attention and investment. Regular training, awareness campaigns, and security audits are just a few examples of the ongoing efforts that are necessary to maintain a strong cybersecurity culture.

In summary, the optimal time for building a cybersecurity culture in TVET colleges is as soon as possible, with a focus on making it a continuous process that is integrated into the college's overall culture and operations.

ADMINISTERING THE INTERVENTION PROGRAMME

There are several considerations regarding administering the programme of the cybersecurity culture intervention (based on NSIT SP 800-12):

- **Visibility** will be of key importance for the success of the intervention. Achieving a prominent place in the selected colleges should begin during the early stages of the intervention programme.
- **Methods**, i.e. the choice of delivery methods should be consistent with the material presented, which we will tailor to the specific needs of the selected colleges' teachers, managers, and students.
- **Topics** should be selected based on the requirements of the intervention's participants at the selected institutions.

- **Materials** should be of optimal high quality to avoid unnecessary costs of developing near-perfect material from afresh. This should be agreed upon with the selected college participants in this intervention.
- **Presentation** considerations are linked to the frequency of training, the length of the presentation, and the style of presentation. This will be done in agreement with the stakeholders.

All these issues should include the intervention implementers (INSETA and DUT) and managers, teachers, and students.

THE STREAMLINED DEVELOPMENT OF CYBERSECURITY CULTURE IN TEVT COLLEGES

The complexity comes in various forms such are technical, environmental, organisational, or social. Often complex implementation models do not have a chance to succeed due to the many variables to be measured, such as the dose of the Business Process Management Challenges (Chapela-Campa Manuel et al., 2019) - like the process of changing cybersecurity culture. The issue involves a process, such as changing cybersecurity culture, which can often be portrayed as the system's dynamics in space and time in which unexpected change takes place, new objects emerge, and existing objects transform (Batty & Torrens, 2001).

As this research is related to the TVET colleges in South Africa representing an uncharted territory, it is expected that some unexpected changes can take place during the implementation of the intervention. Project management, including interventions, is about people and not about tools (Johns, 2008) so the implementation teams should mind the fact that it is dealing with a different, heterogeneous group of people: managers, teachers, and students. Furthermore, for a complex intervention to succeed, it must be bounded in space and time (Epstein, 1999). Hence, the streamlined intervention should optimally last one year (two semesters) or a minimum of one semester.

The streamlined intervention includes streamlining the curriculum to be delivered by selecting and agreeing on an optimal number of themes or subjects to be thought about. As of 2022, TVET colleges introduced two new cybersecurity culture-related subjects "Introduction to Cybersecurity" and "Computer practice", these can be used as the curriculum bases for building cybersecurity culture. However, in agreement with the relevant teachers, some other appropriate themes can be added such as those discussed in Chapter 4, section "Improving cybersecurity culture through education: Cybersecurity culture curriculum".

The development of the cybersecurity culture should be complemented by organising and deploying at least two cybersecurity culture awareness campaigns per semester. These campaigns should, among others, include the preparation of the relevant material, communication, events, and behaviour testing (e.g. Winkler & Manke, 2013; Bada & Sasse, 2014). The latter will be done inside the monitoring and evaluation of the whole intervention.

The reviewed literature reported in this document points out that knowledge and awareness play a crucial role in building an appropriate cybersecurity culture. For example, Laycock et al. (2019) believe that if a person is not aware of basic concepts of cybersecurity, he or she is more prone to security threats than others. Hence, knowledge, gained through curriculum and awareness campaigns, is one of the key concepts in the research and practice of human factors in cybersecurity (Herath & Rao, 2009; ENISA, 2010).

Minding the above and the current state of cybersecurity culture at the researched colleges, we believe that streamlining the project in the described way will make the implementation of the cybersecurity culture in TVET colleges manageable, hence significantly increasing the project's chinches of success.

This streamlining should not impede the validity and usefulness of the proposed intervention as it will bring a unique insight into the key elements impacting the cybersecurity culture of TEVT colleges in South Africa. It is also expected that this pioneering, streamlined implementation will also be a base for exploring the influence of other elements of cybersecurity culture on the security practices at TVET colleges.

POSSIBLE IMPLEMENTATION HURDLES

The reviewed literature (e.g. Civilcharran, 2020) suggest that possible implementation hurdles can appear. Considering and removing these hurdles will heel the successful implementation of the entire programme.

INSUFFICIENT TIME TO COVER THE CURRICULUM

Since much time is required to address the shortfall of students entering the university with inadequate knowledge of generic digital skills, including cybersecurity, there is insufficient time to cover all fundamental aspects of these skills. Given the fact that there are a vast number of cybersecurity skills that are considered fundamental to the successful functioning of a society and industry, the current time allocation for the teaching and learning of many essential digital skills is inadequate.

INADEQUATE RESOURCES AVAILABLE

Many participants in this study have pointed out that their institutions are under-resourced, especially when teaching digital proficiencies, which is either due to inadequate funding or their class sizes (e.g. owing to the high intake of students). Consequently, these institutions need to find ways to improve their resources and relook at their teaching styles/methods, in addition to providing the necessary computer resources to facilitate a teaching methodology that suits the needs of the discipline.

STAFFING ISSUES

Some lecturers still have inadequate knowledge and training in digital skills in general and cybersecurity, and for that reason, they may be reluctant to integrate some digital skills that the industry requires into the curricula. Once individuals join HEIs as academics, there is little or no incentive for them to up-skill in line with industry trends or their institutional needs. If staff do not have any inclination to update the skills and methodologies that they teach, it can be a tremendous challenge. However, it seems that there is currently no authentic way that the HEIs can enforce academics to upskill.

LACK OF POLICIES AND PROCEDURES

The current academic climate reveals a lack of policies and procedures at the institutional level to promote the alignment of digital skills, including cybersecurity, and curricula to industry requirements, a challenge that has not yet been addressed. Several institutional challenges discussed in this section may be solved completely or to a certain degree, by resolving this challenge, that is a lack of policies and procedures.

CHAPTER 8: CONCLUSION AND RECOMMENDATIONS

Assessing the level of cybersecurity culture in TVET colleges in South Africa before this research was challenging due to the lack of available data and the wide variation in cybersecurity practices across these institutions in South Africa. However, there was evidence that suggested that many TVET colleges face significant cybersecurity challenges and may lack the resources and expertise to adequately address them. A survey conducted by the South African Banking Risk Information Centre (SABRIC) in 2019 found that only 24% of the surveyed organisations, including TVET colleges, had implemented basic cybersecurity measures such as firewalls and anti-virus software. This suggested that many TVET colleges may not have the necessary security infrastructure and skills in place to protect against cyber threats.

Furthermore, the 2020 report by the Department of Higher Education and Training (DHET) found that many TVET colleges lacked cybersecurity policies and procedures and did not have formal cybersecurity training programs for staff and students. The report also noted that TVET colleges faced significant challenges in securing their network infrastructure due to limited resources and technical expertise (DHET, 2020). All of the above prompted the Insurance Sector Education and Training Authority (INSETA) to commission the research to the Durban University of Technology (DUT) aimed at building a cybersecurity culture in TVET colleges in South Africa.

The motivation for conducting this research lies in the fact that the threats to the security of digital systems are constantly evolving, hence requiring proper awareness education and training. The justification of this statement comes from Tasevski's (2013) research, which argues that only significant changes in user perception, culture and education can effectively reduce the number of cybersecurity breaches. Hence, the intervention proposed by this study is aimed at raising the awareness and cultural levels of students, teachers, managers, and admin staff at TVET colleges that use digital technologies for teaching, learning and in everyday life.

This research was divided into two phases: creating the conceptual model for building a cybersecurity culture, and implementing an intervention based on the model derived from this study. The first phase was accomplished by an in-depth review of academic literature and industry reports. The created "Conceptual implementation model for developing cybersecurity culture in TVET colleges" was then used to assess the current state of cybersecurity culture in the two selected colleges. This was done by disseminating a qualitative questionnaire to the participants and organising two focus groups. The study included students, teachers, and managers at the studied institutions: Umfolozi and Elangeni TVET colleges. The foundation for the second phase (i.e. intervention) is prepared by this study and the implementation is planned for the coming school years.

The analysis of the literature review and the resulting "Conceptual implementation model for cybersecurity culture in TVET colleges" have theoretically answered the main research question "What are crucial elements of an Action plan for building cybersecurity culture in TVET colleges and how these elements can be effectively integrated to form an executable Action plan" through conceptually answering the sub-questions: "What are crucial elements of an Action plan for building cybersecurity culture in TVET colleges from the students' and teachers' perspectives" and "How these elements can be effectively integrated to form an executable Action plan".

The third question, i.e. "What is the way of effectively executing such an Action plan to increase cybersecurity culture among students at TVET colleges in South Africa" is also answered theoretically by giving the implementation guidelines, which can be used for the development of an actual action plan for building cybersecurity culture in TVET colleges in South Africa. The final answer to the main research question will come after the implementation phase of this study, which should confirm the useability of the intervention proposed by this study.

Answering the research questions has consequently resulted in meeting the main objectives of this study, which was "To identify and define crucial elements of Conceptual model for building cybersecurity culture in TVET colleges, and to devise an appropriate Action plan", though reaching sub-objectives "To identify and define crucial elements of Conceptual model for building cybersecurity culture at TVET colleges", "To explore an effective way of integrating these elements into the form of an executable Action plan", and "To define a way of effectively executing such an Action plan to increase cybersecurity culture in TVET colleges in South Africa".

Although this study has already positively impacted cybersecurity awareness at the selected colleges, the future works related to this study are about making a considerable cybersecurity **impact** - not only on the cybersecurity posture of the participating TVET colleges but also on the cybersecurity culture of the surrounding communities. It will involve the implementation of the intervention aimed at developing a cybersecurity culture in the selected TVET colleges and measuring the success of the implementation. If successful, the same or similar intervention can be emulated by other TVET colleges in South Africa. The implementation of the model in selected colleges should follow the evaluation of the intervention and adjust the model, based on the monitoring and evaluation reports.

The limitation of this study is related to the participation of the respondents from the selected colleges. Namely, not as many managers, teachers, and students as planned were willing to participate in the surveys and focus groups. This was remedied by a discussion with the respondents about cybersecurity culture at various other gatherings (i.e. lectures and seminars) aimed at the research capacitating of the lecturers and managers at the studied institutions. Since the patterns in the responses were very much repetitive, the DUT research team believes that these limitations did not affect the validity of this study.

Being pioneering, this research concentrated mainly on the role of cybersecurity education and awareness campaigns. Although touching on other topics, due to the limited time and resources, this study could not extensively explore several other variables that influence building cybersecurity cultures such as in-depth exploring cybersecurity risk management, strategy, policies, and practices required for building a sound cybersecurity culture in TVET colleges. These explorations are recommended for future studies.

REFERENCES

Advenica (2020) Security culture - an important part of cybersecurity, [online] https://advenica.com/en/blog/2020-01-23/security-culture-an-important-part-of-cybersecurity

Aguilar, F.J. (1967) Scanning the Business Environment, Macmillan

Ajzen, I., & Fishbein, M. (2005) The influence of attitudes on behavior, The handbook of attitudes 173 (221), 31

Albrechtsen, E. & Hovden, J. (2010) Improving information security awareness and behaviour through dialogue, participation and collective reflection, An intervention study, Computers & Security, 29(4), p.432–445

AlHogail, A. (2015) Design and validation of information security culture framework. Computers in Human Behavior, 49, 567-575

AlHogail, A. (2017) Managing Human Factor to Improve Information Security in Organization

Al-Izki, F. & Weir, G.R.S. (2016) Management attitudes toward information security in Omani public sector organizations, 2016 Cybersecurity and Cyberforensics Conference

AlKalbani, A., Deng, H., & Kam, B., (2014) A Conceptual Framework for Information Security in Public Organizations for E-Government Development, in Felix B Tan, Deborah Bunker (ed.) Proceedings of the 25th Australasian Conference on Information Systems (ACIS 2014) 1-11

AlKalbani, A., Deng, H., Kam, B., & Zhang, X. (2017) Information Security compliance in organizations: an institutional perspective, Data and Information Management, 1(2), 104-114

Alman, D. (2013) Human Activity System (HAS) Mapping, [online] https://www.slideshare.net/davidalman/human-activity-system-has-mapping

Alnatheer, M.A. Chan, T. & Nelson, K. (2012) Understanding and Measuring Information Security Culture, The Pacific Asia Conference on Information Systems (PACIS), 11-15July, Ho Chi Minh City, Vietnam

Al-shehri, Y. (2012) Information Security Awareness and Culture, British Journal of Arts and Social Sciences, vol. 6, no. 1, pp. 61–69, 2012

Ardichvili, A., Page, V. & Wentling, T. 2003) Motivation and barriers to participation in virtual knowledge-sharing communities of practice, Journal of Knowledge Management 7 (1)

Arhin, K. & Wiredu, G. O. (2018) An Organizational Communication Approach to Information Security, The African Journal of Information Systems, 10(4), 1

Ashenden, D. (2008) Information Security management: A human challenge? Information Security Technology Report, vol. 13, no. 4, pp. 195–201, Nov. 2008

Ashenden, D. & Sasse, A. (2013) CISOs and organizational culture: Their own worst enemy? Computers & Security 39, 396-405

Backhouse, J. & Dhillon, G. (1996) Structures of responsibility and security of information systems, European Journal of Information Systems, 5:1, 2-9

Bada, M. & Sasse, A. (2014) Cyber Security Awareness Campaigns: Why do they fail to change behaviour? Global Cyber Security Capacity Centre: Draft Working Paper, University of Oxford

Bada, M., Sasse, A. M. & Nurse, J. R. (2015) Cyber security awareness campaigns: Why do they fail to change behaviour? The International Conference on Cyber Security for Sustainable Society, United Kingdom

Bada, M., Von Solms, B. & Agrafiotis, I. (2019) Reviewing national cybersecurity awareness in Africa: an empirical study, The Third International Conference on Cyber-Technologies and Cyber-Systems, CYBER, Athens, Greece

Bandara, I., Ioras, F. & Maher, K. (2014) Cyber security concerns in e-learning education, Proceedings of ICERI2014 Conference 17th-19th November 2014, Seville, Spain

Barton, K.A., Tejay, G., Lane, M. & Terrell, S. (2016) Information system security commitment: A study of external influences on senior management, Computers & Security 59, 9-25

Basinger, J. (2019) A Campus Culture of Cybersecurity, The Chronicle of Higher Education, Inc, [online] https://library.educause.edu/resources/2019/3/a-campus-culture-of-cybersecurity

Batty, M. & Torrens, P.M. (2001) Defining Complexity, Modeling Complexity, Colloquium on "Living with Limits to Knowledge", the Central European University, Budapest

Beautement, A., Sasse, A. & Wonham, M. (2008) The compliance budget: managing security behaviour in organisations, Research Gate, [online] https://www.researchgate.net/publication/228731426_The_compliance_budget_managing_security_behaviour_in_organisations

Bennett, A. Elma, C. (2006) Qualitative research: Recent Developments in Case Study Methods, Annual Review of Political Science 9, 1 (2006), 455–476

Bernik, I. & Prislan, K. (2016) Measuring information security performance with 10 by 10 model for holistic state evaluation, PLoS ONE 11 (9)

Beveridge, R. (2020) Effectiveness of Increasing Realism Into Cybersecurity Training, International Journal of Cyber Research and Education 2(1):40-54

Bhana, N. (2020) Operational impact of the coronavirus on the insurance industry, in Resilience The South African Insurance Industry Survey 2020, KPMG, September 2020, [online] https://assets.kpmg/content/dam/kpmg/za/pdf/pdf2020/south-african-insurance-survey-2020.pdf

Bicchieri, C. (2016) Norms in the wild: How to diagnose, measure, and change social norms, Oxford University Press

Bishop, C. (2019) Enabling young rural women to participate in rural transformation in East and Southern Africa, Food and Agriculture Organization of the United Nations, [online] http://www.fao.org/3/CA3434EN/ca3434en.pdf

Branson, N., Hofmeyr, C., Papier, J., & Needham, S. (2015). Post-school education: Broadening alternative pathways from school to work, South African Child Gauge, 1, 1–8

Brantlinger, E., Jimenez, R., Klingner, J. Pugach, M. & Richardson, V. (2005) Qualitative studies in special education, Exceptional Children 71, 2 (2005), 195–207

Brewerton, P. & Millward, L. (2002) Organizational Research Methods, London: Sage

Bryman, A. & Bell, E. (2011) “Business Research Methods” 3rd edition, Oxford University Press

Burns, A. (2009) Action Research in Qualitative Research in Applied Linguistics: A Practical Introduction (Eds. Heigham, J. & Croker, R.A.), Palgrave Macmillan

Burrell, G. & Morgan, G. (2017) Sociological paradigms and organisational analysis: Elements of the sociology of corporate life, Routledge

Business Insider (2019) Chinese hackers targeted University of Pretoria in search of military technology, March 28, 2019, Online: https://www.businessinsider.com/chinese-hackers-targeted-south-african-university-for-military-technology-2019-3

Cape Talk (2021) Impersonator fraud rose by 337% in 2020 - here's how to protect your identity, [online] https://www.capetalk.co.za/articles/410285/identity-fraud-rose-by-over-330-in-2020-here-s-one-way-to-protect-yourself-from-impersonators#:~:text=Impersonation%20fraud%20has%20increased%20by,fraud%20over%20the%20past%20year

Chapela-Campa Manuel, D., Mucientes, M. & LamaM. (2019) Simplification of Complex Process Models by Abstracting Infrequent Behaviour, International Conference on Service-Oriented Computing, Toulouse, France, Volume: 11895

Careers Portal (2022) Thousands Of Graduates To Be Placed In Learning Programmes, [online] https://www.careersportal.co.za/news/thousands-of-graduates-to-be-placed-in-learning-programmes#:~:text=Higher%20Education%20Minister%20Dr.,580%20849%20in%202022%2F23.

CCIS (2021) The relationship between ICT security, cyber security and information security, Center for Cyber and Information Security, online] https://ccis.no/cyber-security-versus-information-security/

Chatterjee, D. (2019) Should executives go to jail over cyber security breaches? Journal of Organizational Computing and Electronic Commerce, Vol. 29 No. 1, pp. 1-3

Chatterjee, C. & Sokol, D. D. (2019) Data Security, Data Breaches, and Compliance, In Sokol & v. Rooij (Eds.), Cambridge Handbook on Compliance

Check Point (2021) As battle against cybercrime continues during cybersecurity awareness-month [online] https://blog.checkpoint.com/2021/10/06/as-battle-against-cybercrime-continues-during-cybersecurity-awareness-month-check-point-research-reports-40-increase-in-cyberattacks/

Christiansen, B. (2014) Handbook of Research on Effective Marketing in Contemporary Globalism, IGI Global

CISA (2022) Executive order on improving the nation’s cybersecurity, Cybersecurity & Infrastructure Security Agency, [online] https://www.cisa.gov/executive-order-improving-nations-cybersecurity

Civilcharran, S. (2020) Digital skills preparedness of higher education students for the "Real Estate, Finance and Business" sector in South Africa, Doctoral thesis at the University of Kwazulu-Natal

CNET (2022) Average Data Breach Costs Hit a Record $4.4 Million, Report Says, [online] https://www.cnet.com/tech/services-and-software/average-data-breach-costs-hit-a-record-4-4-million-report-says/

Colleges Education (2021) Vulnerabilities and Preventing Attacks, [online] https://collegiseducation.com/news/technology/cybersecurity-higher-ed-understanding-vulnerabilities-preventing-attacks/

Colicchia, C., Creazza, A. & Menachof, D.A. (2019) Managing cyber and information risks in supply chains: insights from an exploratory analysis, Supply Chain Management: An International Journal 24, 2 (March 2019), 215–240

Collins English Dictionary (2020) HarperCollins Publishers, 2020

Collins, C.S. & Stockton, C.M. (2018) The Central Role of Theory in Qualitative Research, International Journal of Qualitative Methods, Volume: 17, Issue: 1

Cone, W. D., Irvine, C. E., Thompson, M. F. &Nguyen, T. D. (2007) A video game for cyber security training and awareness, Computers & Security 26, 63 – 72

Connolly, L. & Lang, M. (2012) Investigation of Cultural Aspects within Information Systems Security Research, The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012)

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013) Future directions for behavioral information security research, Computers & Security, 32, 90-101

CSIS (2011) Cybersecurity Two Years Later, Center for Strategic and International Studies, [online] https://doi.org/978-0-89206-625-4

Cuganesan, S., Steele, C. & Hart, A. (2018) How senior management and workplace norms influence information security attitudes and self-efficacy, Behaviour & Information Technology, 37(1), 50-65

Cybercrime Bill (2016) Cybercrimes and Cybersecurity Bill, Minister of Justice And Correctional Services, Government Gazette No. 40487 of 9 December 2016

Da Veiga, A. (2016) A Cybersecurity Culture Research Philosophy and Approach to Develop a Valid and Reliable Measuring Instrument, SAI Computing Conference 2016, London, UK Volume: 2016

Das, S., Hyun-Jin Kim, T., Dabbish, L.A. & Hong, J.I. (2014) The Effect of Social Influence on Security Sensitivity, The Tenth Symposium on Usable Privacy and Security (SOUPS) took place July 9-11, 2014, at Facebook Headquarters in Menlo Park, California

da Veiga, A. & Martins, N. (2015) Information security culture and information protection culture: A validated assessment instrument, Computer Law & Security Review 31(2)

da Veiga, A. (2016) A cyber- security culture research philosophy and approach to developing a valid and reliable measuring instrument, SAI Computing Conference 2016, 2016, p. 10

Deloitte (2018) Elevating cybersecurity on the higher education leadership agenda, EDUCAUSE, [online] https://www2.deloitte.com/us/en/insights/industry/public-sector/cybersecurity-on-higher-education-leadership-agenda.html

De Maggio, M.C., Mastrapasqua, M., Tesei, M., Chittaro, A. & Setola, R. (2019) How to improve the security awareness in complex organizations, European Journal of Scientific Research, Vol. 4, pp. 33-49

DHET (2017) National skills development plan, Department of Higher Education and Training

DHET (2020) Cybersecurity readiness of South African higher education institutions, Department of Higher Education and Training, Online: https://www.gov.za/sites/default/files/gcis_document/202011/43807gon1375.pdf

Ditsa, G. (2003) Executive Information Systems Use in Organisational Contexts: An Exploratory User Behaviour Testing, Information Management: Support Systems & Multimedia Technology IRM Press London, 2003, pp109-155

Dowd, J. (2016) Building a Business Case for Effective Security Awareness Training, [online] https://info.phishlabs.com/blog/building-a-business-case-for-effective-security-awareness-training

Driscoll, A. (2009) Carnegie's New Community Engagement Classification: Affirming Higher Education's Role in Community, New Directions for Higher Education, No. 147, Wiley

Dudovskiy, J. (2022) The Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-Step Assistance (6th edition), Business Research Methodology

EdTech (2018) 3 Cybersecurity Focus Areas for Education Institutions in 2019, [online] https://edtechmagazine.com/higher/article/2018/12/3-cybersecurity-focus-areas-education-institutions-2019

Emisoft (2019) The State of Ransomware in the US: Report and Statistics 2019, [online] https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

ENISA (2010) The new users' guide: How to raise information security awareness, [online] https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide/at_download/fullReport

ENISA (2018) Cyber Security Culture in organisations, European Union Agency for Network and Information Security [online] https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations/at_download/fullReport#:~:text=Cybersecurity%20Culture%20(CSC)%20of%20organizations,behaviour%20with%20information%20technologies

Enz, C. (2009) Hospitality Strategic Management: Concepts and Cases, Wiley Publishing

Epstein, J. M. (1999) Agent-Based Computational Model and Generative Social Science, Complexity, 4, 41-60

Ernst & Young (2017) Cyber Strategy for Insurers, Managing physical and digital assets to protect brand and reputation, [online] https://www.ey.com/Publication/vwLUAssets/ey-cyber-strategy-for-insurers/$File/ey-cyber-strategy-for-insurers.pdf

FAO (2020) 5 ways we can enable young #ruralwomen to participate in rural transformation, Food and Agriculture Organisation of the United Nations, [online] http://www.fao.org/fao-stories/article/en/c/1263688/

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015) Information security awareness in educational institution: An analysis of students' individual factors, In Trustcom/BigDataSE/ISPA, 2015 IEEE (Vol. 1, pp. 352-359)

Fischer, J. C. (2001) Action research rationale and planning: Developing a framework for teacher inquiry, in G. Burnaford, J. C. Fischer, & D. Hobson (Eds.), Teachers doing research: The power of action through inquiry (pp. 29–48), Mahwah, NJ: Lawrence Erlbaum Associate

Fletcher, A.J. & Marchildon, G.P. (2014) Using the Delphi Method for Qualitative, Participatory Action Research in Health Leadership, International Journal of Qualitative Methods 13, 1 (Feb 2014), 1–18

Flinders, D. J. & Mills, G. E. (1993) Theory and concepts in qualitative research: Perspectives from the field, New York, NY: Teachers College

Flores, W.R., Antonsen, E. & Ekstedt, M. (2014) Information security knowledge sharing in organizations: investigating the effect of behavioral information security governance and national culture, Computers & Security, 43, 90-110

Fujs, D., Mihelic, A. & Vrhovec, S.L.R. (2019) The power of interpretation: Qualitative methods in cybersecurity research, In Proceedings of the 14th International Conference on Availability, Reliability and Security, (ARES 2019) (ARES '19), August 26–29, 2019, Canterbury, United Kingdom

Furnell, S. (2008) End-user security culture: a lesson that will never be learnt? Computer Fraud Security, No. April, 2008

Furnell, S. & Thomson, K.L. (2009) From culture to disobedience: Recognising the varying user acceptance of IT security, Computer Fraud & Security, vol. 2009, no. 2, pp. 5–10

Gavrilets, S. & Richerson, P. J. (2017) Collective action and the evolution of social norm internalization, Proceedings of the National Academy of Sciences, 114(23), 6068-6073

Gcaza N., Solms R. & Vuuren J. (2015) An Ontology for a National CyberSecurity Culture Environment, In Proceedings of the 9th International Symposium on Human Aspects of Information Security & Assurance (1-10)

Gcza, N. & van Solms, R. (2017) A strategy for a cybersecurity culture: A South African perspective, The Electronic Journal of Information Systems in Developing Countries (EJISDC) 80, 6, 1-17

Gcaza, N. & von Solms, R. (2017a) Cybersecurity Culture: An ill-defined Problem, Information Security Education for a Global Digital Society pp 98-109

Glen, S. (2013) Qualitative Variable (Categorical Variable): Definition and Examples, [online] https://www.statisticshowto.com/qualitative-variable/

Global Banking and Finance Review (2018) TOP STORIES: Data breaches top list of concerns for insurance industry, [online] https://www.globalbankingandfinance.com/data-breaches-top-list-of-concerns-for-insurance-industry/

Goldman, G. & Nieuwenhuizen, C. (2006) Strategy: Sustaining Competitive Advantage in a Globalised Context, Juta and Company Ltd

Gonzalez, J. J. & Sawicka, A. (2002) A framework for Human Factors in Information Security.Presented at the 2002 WSEAS International Conference on Information Security, Rio de Janeiro,2002

Grobler, M., Dlamini, Z., Ngobeni, S. & Labuschagne, A. (2011) Towards a Cyber security aware rural community, Conference: Information Security South Africa Conference 2011, Hyatt Regency Hotel, Rosebank, Johannesburg, South Africa, August 15-17, 2011

Guba, E. G. & Lincoln, Y. S. (1994) Competing paradigms in qualitative research, In Denzin, N. K., Lincoln, Y. S. (Eds.), Handbook of qualitative research (pp. 105–117), London, England: Sage

Haag, S. & Cummings, M. (2013) Management of Information Systems for the Information Age, 9th ed., New York: McGraw-Hill Irwin, 2013

Hadlington, L. J. (2018) Employees Attitudes towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom, International Journal of Cyber Criminology, 12(1)

Halevi, T., Memon, N., Lewis, J., Kumaragury, P. & Arora, S. (2016) Cultural and psychological factors in cyber-security, Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services, November 2016

Hatch, M.J. (1993) The dynamics of organizational culture. The Academy of Management Review 18, 657-693

Hechter, M. & Opp, K. D. (2001) Social norms, Russell Sage Foundation

Hearth, T., & Rao, H. R. (2009) Protection motivation and deterrence: a framework for security policy compliance in organizations, European Journal of Information Systems, 18(2), 106-125

Hedström, K., Kolkowska, E., Karlsson, F. & Allen, J.P. (2011) Value conflicts for information security management, Journal of Strategic Information Systems 20, 373-384

Holland, B. & Ramaley, J.A. (2008) Creating a Supportive Environment for Community-University Engagement: Conceptual Frameworks, In Engaging Communities, Proceedings of the 31st HERDSA Annual Conference, 1-4 July 2008, Rotorua, New Zealand.

Hong, J., Das, S., Hyun-Jin Kim, T. & Dabbish, L. (2015) Social Cybersecurity: Applying Social Psychology to Cybersecurity, Human Computer Interaction Consortium, Carnegie Mellon University

Howell, D. C. (2014) Fundamental Statistics for the Behavioral Sciences, 8th Ed., Belmont CA: Wadsworth Cengage Learning

Huang, K. & Pearlson, K. (2019) Building a Model of Organizational Cybersecurity Culture, MIT CAMS – Organizational Cybersecurity Culture, [online] http://web.mit.edu/smadnick/www/wp/2020-05.pdf

Huda, S. (2019). Next Level Cybersecurity: Detect the signals Stop the Hack, Leader-Press

IBM (2018) 2018 Cost of Data Breach Study: Impact of Business Continuity Management, Ponemon Institute [online] https://www.ibm.com/downloads/cas/AEJYBPWA

IBM (2020) How much would a data breach cost your business? [online] https://www.ibm.com/security/data-breach

IBM (2022) IBM Report: South African data breach costs reach all-time high, [online] https://www.biztechafrica.com/article/ibm-report-south-african-data-breach-costs-reach-a/17008/

ICASA (2020) The State of the ICT Sector Report in South Africa 2020, [online] https://www.icasa.org.za/uploads/files/State-of-the-ICT-Sector-Report-March-2020.pdf

IFAD (2019) Rural Development Report 2019, [online] https://www.ifad.org/en/web/knowledge/publication/asset/41173272

IGF (2018) Cybersecurity Culture, Norms and Values, Internet Governance forum, [online] https://www.intgovforum.org/multilingual/filedepot_download/6764/1401

ILO (2020) The Digitization of TVET and Skills Systems, International Labour Organisation, [online] https://www.ilo.org/wcmsp5/groups/public/---ed_emp/---emp_ent/documents/publication/wcms_752213.pdf

IOL (2022) Cyber security: Universities under fire, Online: https://www.iol.co.za/business-report/economy/cyber-security-universities-under-fire-42481925-60dc-439c-86a1-13eabd30121c

Impact (2019) Why a Disaster Recovery Plan Is Vital for SMBs, [online] https://www.impactmybiz.com/blog/blog-why-a-disaster-recovery-plan-is-vital-for-smbs/

Impact (2021) 15 Cybersecurity In Education Stats You Should Know, [online] https://www.impactmybiz.com/blog/cybersecurity-in-education-stats/

Inc (2018) How Can 73 Percent of Companies Not Be Prepared for Hackers? [online] https://www.inc.com/adam-levin/more-than-70-percent-of-businesses-admit-theyre-unprepared-for-a-cyberattack.html

IOL (2020) Data breach costs SA companies R40.2 million average in 2020, [online] https://www.iol.co.za/business-report/companies/data-breach-costs-sa-companies-r402-million-average-in-2020-6649ae0a-b803-482c-978f-b395517c7fa7#:~:text=2%20million%20average%20in%202020,-By%20Sizwe%20Dlamini&text=JOHANNESBURG%20%E2%80%93%20IBM%20Security%20this%20week,on%20average%20among%20organisations%20studied

Ismail, W.B.W. & Yusof, M. (2018) Mitigation strategies for unintentional insider threats on information leaks, International Journal of Security and Its Applications 12, 37-46

ITouch (2021) 78% MOBILE USERS GROWTH EXPECTED BY 2022, [online] https://itouch.co.za/news/mobile-growth-in-sa.php

ITU (2009) Global Security Report 2009, International Telecommunication Union

IvyPanda (2022) Cyber Security Threats: How Students Can Protect Their Data, [online] https://ivypanda.com/blog/cyber-security-threats/

Jackson, C. (2020) Insurance and reinsurance in South Africa: overview, [online] https://uk.practicallaw.thomsonreuters.com/1-505-2026?transitionType=Default&contextData=(sc.Default)&firstPage=true

Jhangiani, R., Tarry, H. & Stangor, C., (2014) Principles of Social Psychology-1st International Edition, [online] https://opentextbc.ca/socialpsychology/chapter/exploring-attitudes/

Johns, T.G. (2008) The art of Project Management and Complexity, PMI Global Conference Proceedings, 2008, Denver, Colorado

Kabanda, G. (2018) A Cybersecurity Culture Framework and Its Impact on Zimbabwean Organizations, Asian Journal of Management, Engineering & Computer Sciences, Vol. 3(4), October 2018: 17-34

Karyada, M., Kiountouzis, E. & Kokolakis, S. (2005) Information systems security policies: A contextual perspective. Computers & Security 24, 246-260

Kaspersky (2018) What is Cyber Security? [online] https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kaspersky (2020) What cybersecurity trends should you look out for in 2020? [online] https://www.kaspersky.com/blog/secure-futures-magazine/2020-cybersecurity-predictions/32068/

Kaur, J. & Mustafa, N. (2013) Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME, Research and Innovation in Information Systems (ICRIIS), 2013 International Conference

Kavak, H., Padilla, J.J., Vernon-Bido, D., Diallo, S.Y., Gore, R. & Shetty, S. (2021) Simulation for cybersecurity: state of the art and future directions, Journal of Cybersecurity, Volume 7, Issue 1, 2021

Kearney, W.D. & Kruger, H.A. (2016) Can perceptual differences account for enigmatic information security behaviour in an organization? Computers & Security 61, 46-58

Kellogg Commission (1999) Kellogg Commission on the Future of State and Land-Grant Universities, Returning to our roots, Third Report, Washington, DC: National Association of State Universities and Land-Grant Colleges

Kim, D.J., Hwang, I.H. & Kim, J.S., (2016) A Study on Employee's Compliance Behavior towards Information Security Policy: A Modified Triandis Model. Journal of Digital Convergence, 14(4), 209-220

Kissel R. (2013) Glossary of Key Information Security Terms, National Institute of Standards and Technology, 2013

Knapp, K. J., Morris Jr., R.F., Marshall, T.E. & Byrd, T.A. (2009) Information security policy: An organizational-level process model. Computers & Security 28, 493-508

Kortjan, N. & Von Solms, R. (2014) A conceptual framework for cybersecurity awareness and education in SA, South African Computer Journal, 52, 29-41., vol. 2014, no. 52, pp. 29–41

Lange, R., Hofmann, C. & Di Cara, M.(2020) Guide on making TVET and skills development inclusive for all, International Labour Organisation

Laycock, A., Petric, G. & Roer, K. (2019) The seven dimensions of security culture, CLTRe, Oslo, Norway [online] https://www.knowbe4.com/hubfs/CLTRe-The7DimensionsSecurityCulture-ResearchPaper.pdf

Lacey, D. (2010) Understanding and transforming organizational security culture, Information Management & Computer Security, Vol. 18 No. 1, pp. 4-13

Leenen, L., van Vuren, J.J. & van Vuren, A-M.J. (2020) Cybersecurity and Cybercrime Combatting Culture for African Police Services, Cybersecurity and Cybercrime Combatting Culture for African Police Services. In: Kreps, D., Komukai, T., Gopal, T.V., Ishii, K. (eds) Human-Centric Computing in a Data-Driven Society. HCC 2020. IFIP Advances in Information and Communication Technology, vol 590. Springer

Leidner D.E. & Kayworth, T. (2006) A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict, MIS Quarterly 30(2):357-399

Lewis, J. (2020) What is cybersecurity culture, and how do you build it? [online] https://www.cira.ca/blog/cybersecurity/what-cybersecurity-culture-and-how-do-you-build-it

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019) Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior, International Journal of Information Management, 45:13-24

Lin, C. & Wittmer, J.L.S. (2017) Proactive information security behavior and individual creativity: Effects of group culture and descentralized IT governance, 2017 IEEE International Conference on Intelligence and Security Informatics

Magee, C. S. (2013) Awaiting the cyber 9/11, Joint Force Quarterly, 70, 76–82

Malyuk, A. & Milosavskaya, N. (2016) Cybersecurity Culture as an Element of IT Professional Training, IEEE 2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless

McManners, P. (2015) The action research case study approach: A methodology for complex challenges such as sustainability in aviation, Action Research 14(2)

Mertler, C.A. (2014) Action research: Improving schools and empowering educators, Thousand Oaks, CA: Sage

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C. & Giannakopoulos, G. (2014) The Human Factor of Information Security: Unintentional Damage Perspective, Social and Behavioral Sciences 147, 424 – 428

Mitrovic, Z. (2019) Human factor as a perpetual problem in cybersecurity: Are awareness campaigns wonder drugs? [online] https://vmadvisory.com/human-factor-cybersecurity/

Morris, M. G., Venkatesh, V., & Ackerman, P. L. (2005) Gender and age differences in employee decisions about new technology: An extension to the theory of planned behavior, IEEE Transactions on Engineering Management, 52(1), 69-84

Mungadze, S. (2021) University of Mpumalanga thwarts R100m hack attempt, Online: https://www.itweb.co.za/content/Kjlyrvw1jmmMk6am

MyBroadband (2020) DDoS attacks hit South African universities, Online: https://mybroadband.co.za/news/security/367644-ddos-attacks-hit-south-african-universities.html

National Integrated ICT Policy (2016) National Integrated ICT Policy White Paper, The Department of Telecommunications and Postal Services

NIST (2014) Framework for improving Critical Infrastructure Cybersecurity, Version 1.0, 2014, National Institute of Standards and Technology

NIST (2016) Special Publication 800-160: System Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, Ross et al, November 2016

NIST (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, National Institute of Standards and Technology

NIST (2017) Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, January 10, 2017

NIST SP 800-12 (2017) Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook, National Institute of Standards and Technology, June 2017

Nobles, C. (2022) Stress, burnout, and security fatigue in cybersecurity: a human factors problem, Holistica Journal of Business and Public Administration, Vol. 13, Iss. 1, pp 49-72

Norris, D.F., Mateczun, L., Joshi, A. & Finin, T. (2019) Cyberattacks at the grass roots: American local governments and the need for high levels of cybersecurity, Public Administration Review, Vol. 79 No. 6, pp. 895-904

NSM (2018) Et sikkert digitalt Norge – IKT-risikobilde, Nasjonal sikkerhetsmyndighet

Online Trust Alliance (2018) Cyber Incidents & Breach Trends Reports, Review of and analysis 2017 cyber incidents, trends, and key issues to address

Oxford English Dictionary (20219) Cybercrime [online] https://www.lexico.com/definition/cybercrime

Parry, K., Mumford, M.D., Bower, I. & Watts, L.L. (2014) Qualitative and historiometric methods in leadership research: A review of the first 25years of The Leadership Quarterly, The Leadership Quarterly 25, 1 (Feb 2014), 132–15

Pellissier, R (2008) Business Research Made Easy, Juta and Company Ltd.

Ponemeon (2012) The human factor in data protection, Ponemon Institute [online] https://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf

Porter, G., Hampshire, K., De Lannoy, A., Bango, A., Munthali, A., Robson, E., Tanle, A., Abane, A. & OwusuS. (2018) Youth Livelihoods in the Cellphone Era: Perspectives from Urban Africa, Journal of International Development, V 30:4

Powell, L. & McGrath, S. (2019) Skills for Human Development, Abingdon: Routledge

Pozzebon, M., Mackrell, D. & Nielsen, S. (2014) Structuration bridging diffusion of innovations and gender relations theories: a case of paradigmatic pluralism in IS research, Information Systems Journal, 24(3), pp229-248

Purplesec (2021) 2021 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends, [online] https://purplesec.us/resources/cyber-security-statistics/

Quinn, R.E. (1988) Beyond rational management: Mastering the paradoxes and competing demands of high performance, San Francisco: Jossey-Bass

RAND (2008) Cybersecurity Economic Issues: Corporate Approaches and Challenges to Decisionmaking, [online] https://www.rand.org/pubs/research_briefs/RB9365-1.html

Reegård, K., Blackett, C. & Katta, V. (2019) The Concept of Cybersecurity Culture, 29th European Safety and Reliability Conference (ESREL), Hannover, Germany

Reid, R. & van Niekerk, J. (2014) Towards an Education Campaign for Fostering a Societal, Cyber Security Culture, Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014), 2014, pp. 174–184

Rewire (2022) R2.3.1. Cybersecurity Skills Strategy, Cybersecurity Skills Alliance, [online] https://rewireproject.eu/wp-content/uploads/2022/05/R2.3.1-Cybersecurity-Skills-Strategy_FINAL-v1-compressed.pdf

Roer, K. (2013) The Security Culture Framework, [online] https://securityculturefframework.net

Roer, K. & Petric, G. (2017) Security Culture Report 2017 - In depth insights into the human factor, [online] https://get.clt.re/security-culture-report-2017/

RSA (2017) Translating Security Leadership into Board Value, [online] https://rsa.jiveon.com/community/products/archer-grc/blog/2017/04/25/translating-security-leadership-into-board-value

RSA Conference (2017a) Privacy and Cybersecurity in Education: A Constant Battle, [online] https://www.rsaconference.com/library/blog/privacy-and-cybersecurity-in-education-a-constant-battle

Ruighaver, A.B., Maynard, S.B. & Chang, S. (2007) Organizational security culture: Extending the enduser perspective, Computers & Security 26, 56-62

Rumelt, R. (2011) Good Strategy/Bad Strategy, USA: Profile Books LTD

SA Government Gazette (2015) National Cybersecurity Policy Framework for South Africa, [online] https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf

SABRIC (2019) South African Banking Risk Information Centre: Cybercrime in South Africa 2019, Online: https://www.sabric.co.za/wp-content/uploads/2019/08/SABRIC-Cyber-Crime-Survey-2019.pdf

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015) Information security conscious care behaviour formation in organizations, Computers & Security, 53, 65-78

Sandler, R. (2018) After Studying 6.1 Million Passwords, Researchers Identified the 6 Most Common Mistakes. Take a Look [online] https://www.inc.com/businessinsider/common-password-mistakes-how-to-choose-strongpassword.html

Schein, E.H. (2004) Organizational Culture and Leadership, Jossey-Bass, A Wiley Imprint

Schlienger, T. &Teufel, S. (2005) Tool supported management of information security culture: An application to a private bank, in the 20th IFIP International Information Security Conference (SEC 2005), Security and Privacy in the Age of Ubiquitous Computing, New York: Springer, pp. 65-75

Sentinel One (2022) Cyber Risks in the Education Sector: Why Cybersecurity Needs to Be Top of the Class, [online] https://www.sentinelone.com/blog/cyber-risks-in-the-education-sector-why-cybersecurity-needs-to-be-top-of-the-class/

Shouhuai, X. (2018) Cybersecurity Dynamics: A Foundation for the Science of Cybersecurity, Springer Link

Siponenet, M., Pahnila, S. & Mahmood, M. A. (2010) Compliance with Information Security Policies: An Empirical Investigation, Computer 43 (2): 64–71

Schneider, B. (2012) Participatory Action Research, Mental Health Service User Research, and the Hearing (our) Voices Projects, International Journal of Qualitative Methods 11, 2 (Apr 2012), 152–165

Sophos (2022) The State of Ransomware in Education 2022, [online] https://assets.sophos.com/X24WTUEQ/at/pgvqxjrfq4kf7njrncc7b9jp/sophos-state-of-ransomware-education-2022-wp.pdf

Srinivas, S. & Viljamaa, K. (2008) Emergence of Economic Institutions: Analysing the Third Role of Universities in Turku, Finland, Regional Studies, Volume 42, Issue 3, pp. 323-341

Stanton, J. M., Stam, K. R., Mastrangelo, P. & Jolton, J. (2005) Analysis of end user security behaviors. Computers & Security, 24.2 (2005): 124-133

Steinbart, P.J., Raschke, R.L., Gal, G. & Dilla, W.N. (2018) The influence of a good relationship between the internal audit and information security functions on information security outcomes, Accounting, Organizations & Society, 1-15

Surman, M & Reilly, K. (2003) Sppropriating the internet for social change: towards the strategic use of networked technologies by transnational civil society organizations, Social Science Research Council, November 2003

Tasevski, P. (2013) Methodological approach to security awareness program, Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities, [online] https://www.researchgate.net/publication/279842504_Methodological_approach_to_security_awareness_program?enrichId=rgreq-41a5a01ac67f2c9f88369cb2f94d4dbd-XXX&enrichSource=Y292ZXJQYWdlOzI3OTg0MjUwNDtBUzoyNDg1MDU1MjAzNTczODNAMTQzNjI1OTc0MTg1OQ%3D%3D&el=1_x_3&_esc=publicationCoverPdf

Teh, P., Ahmed, P.K. and D'Arcy, J. (2015) What drives information security policy violations among banking employees?: insights from neutralization and social exchange theory, Journal of Global Information Management, Vol. 23 No. 1, pp. 44-64

Tesone, D.V. (2012) Principles of Management for the Hospitality Industry, Routledge

Thomson, K., von Solms, R., & Louw, L. (2006) Cultivating an Organizational Information Security Culture, Computer Fraud & Security, 2006(10), 7-11

Thsohou, A., Karyda, M. & Kokolakis, S. (2015) Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. Computers & Security 52, 128-141

Torbert, W. R. (1981) "Why Educational Research Has Been So Uneducational: The Case for a New Model of Social Science Based on Collaborative Inquiry", In Reason, P.; Rowan, J. (eds.). Human Inquiry. John Wiley and Sons, pp. 141–151

Tree Solution (2020) Measure the state of a security culture and track its changes, [ONLINE] https://www.treesolution.com/news-english/measure-security-culture-and-changes

Trepper, C. (2006) Training Developers More Efficiently, Information Week Online, www.informationweek.com/738/38addev.htm

Tripwire (2020) Successful Ransomware Attacks on Education Sector Grew 388% in Q3 2020, [online] https://www.tripwire.com/state-of-security/security-data-protection/successful-ransomware-attacks-on-education-sector-grew-388-in-q3-2020/

Tsaia, H.S., Jiang, M., Alhabashbc, S., LaRose, R., Rifon, N.J. & Cotten, S.R. (2016) Understanding online safety behaviors: A protection motivation theory perspective, Computers & Security, Volume 59, June 2016, Pages 138-150

UNECA (2014) United Nations Economic Commission for Africa: Tackling the challenges of cybersecurity in Africa, Policy Brief. No. 002, 6 p. Addis Ababa [online] https://repository.uneca.org/bitstream/handle/10855/22544/b11079411.pdf?sequence=1&isAllowed=y

UNGA (2004) 58/199. Creation of a global culture of cybersecurity and the protection of critical information infrastructures, Fifty-eighth session of General Assembly of the United Nations, New York

UNEVOC (2019) Collaborative research on Community engagement in TVET, Education 2030, The United Nations Education, Scientific and Cultural Organisation, [online] https://unevoc.unesco.org/up/30001-eng.pdf

UNISA (2018) UNISA employee arrested at work by the HAWKS, Online: https://www.unisa.ac.za/static/corporate_web/Content/News%20&%20Media/Media%20releases/documents/Media_Statement_employee_arrested_by_HAWKS.pdf

University World News (2020) South African universities take steps to boost cybersecurity, Online: https://www.universityworldnews.com/post.php?story=20200716131136345

van Niekerk, J. & von Solms, R. (2005) Establishing an Information Security Culture in Organisations: an Outcomes-based Education Approach, [online] https://www.researchgate.net/publication/228947007_Establishing_an_Information_Security_Culture_in_Organisations_an_Outcomes-based_Education_Approach

van Niekerk, J. & von Solms, R. (2005a) A holistic framework for the fostering of an information security sub-culture in organizations, Proceedings of the ISSA 2005 New Knowledge Today Conference, 29 June - 1 July 2005, Balalaika Hotel, Sandton, South Africa

Van Niekerk, J. & Von Solms, R. (2006) Understanding Information Security Culture: A Conceptual Framework, Proc. ISSA 2006, pp. 1–10

Van Niekerk, J. F. & Von Solms, R. (2010) Information security culture: A management perspective, Computer Security, vol. 29, no. 2010, pp. 476–486, Jun. 2010

Venter, I. M., Blignaut, R. J., Renaud, K. & Venter, M. A. (2019) Cyber security education is as essential as "the three R's", Heliyon, 5(12), 1-8

Verizon (2020) 2020 Data Breach Investigations Report, [online] https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Verizon (2022) 2022 Data Breach Investigations Report, [online] https://www.verizon.com/business/resources/reports/dbir/

Von Solms, R. & Van Niekerk, J. (2013) From information security to cyber security, Computer Security, Vol. 2013, no. 38, pp. 97-102

Walaza, M. & Kritzinger, E. (2019) The South African ICT Security Awareness Framework for Education (SAISAFE), Masters thesis, University of South Africa

Wamala, F. (2011) ITU National Cybersecurity Strategy Guide, [online] http://onlinelibrary.wiley.com/doi/10.1002/cbdv.200490137/

Webroot (2017) Cyberthreats to smal-and medium-sized businesses in 2017, [online] https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/2114/9911/0468/SMB-MSP_Survey_US.pdf

Wheelen, T.L. & Hunger, J.D. (2012) Strategic Management and Business Policy: Toward Global Sustainability (13th ed.), Pearson/Prentice Hall

Whitman, M.E. & Mattord, H.J. (2017) Principles of Information Security, Cengage Learning

Williams, B.T. (2014) The joint force commander's guide to cyberspace operations, Joint Force Quarterly, 73(2): 12–19

Willkinson, A., Pettifor, A., Rosenberg, M., Halpern, C., Thirumurthy, H., Collinsen, M. & Khan, K. (2017) The employment environment for youth in rural South Africa: A mixed-methods study, Dev South Afr. 2017; 34(1): 17–32

Winkler, I. & Manke, S. (2013) 7 Reasons for Security Awareness Failure, CSO Magazine, [online] www.csoonline.com/article/2133408/network-security/the-7-elements-of-asuccessful-security-awareness-program.html

World Bank (2021) World Bank Open Data, [online] https://data.worldbank.org/

Yin, R.K. (2017) Case Study Research and Applications: Design and Methods, Sage Publications

Zhang, Z.J., He, W., Li, W. & Abdous, M. (2021) Cybersecurity awareness training programs: a cost–benefit analysis framework, Industrial Management & Data Systems, Vol. 121 No. 3, 2021 pp. 613-636

Zinn, B., Raisch, K. & Reimann, J. (2019) Analysing training needs of TVET teachers in South Africa. An empirical study, International Journal for Research in Vocational Education and Training (IJRVET), Vol.6, Issue 2, August 2019, 174-197

Zulu, W.V. & Mutereko, S. (2020) Exploring the Causes of Student Attrition in South African TVET Colleges: A Case of One KwaZulu-Natal Technical and Vocational Education and Training College, Springer Nature B.V. 2020

APPENDIX A: TIPS FOR INFLUENCING THE DIMENSIONS OF CYBERSECURITY CULTURE

These tips are given by Laycock et al (2019):

TIPS FOR POSITIVELY INFLUENCING ATTITUDES TOWARDS SECURITY IN THE ORGANISATION

An attitude is likely to be stronger if there is direct experience. Attitudes can be changed by reinforcing positive norms and through effective communication. We recommend using techniques such as:

1. Celebrating achievements (See Norms)
2. Acknowledging concerns (See Communication)
3. Involving other members of the organization in planning (See Responsibilities)
4. Exemplifying behaviours by sharing examples of correct and desired behaviour (See Behaviours)
5. Empowering employees by providing adequate tools and processes (See Compliance)

TIPS FOR POSITIVELY INFLUENCING BEHAVIOURS

Employee behaviour is empirically dependent on the dimensions of security culture:

1. Normal behaviour in social settings has a strong influence on acceptable behaviour in an organization (See Norms)
2. Different training methods may change our behaviour of certain issues (See Attitudes)
3. Implement short communications that are easily available to the employee (See Communication)
4. Identify processes that are important and assess employees' knowledge of their existence (See Cognition)
5. Information security policies guide all employees on what behaviour is expected and how to conform (See Compliance)

TIPS FOR POSITIVELY INFLUENCING COGNITION

Whilst knowledge by itself is unlikely to have a direct impact on behaviour, the cognitive processes required to acquire knowledge related to security have a direct and indirect influence on other dimensions that are significant to improving security culture:

1. Establish clear expectations from the start (See Norms and Compliance)
2. Emphasize the important role that each employee has in sustaining the security of the organization (See Responsibilities)

3. Share stories that advertise the security-related social norms and support a sense of belonging (See Communication and Norms)
4. Ensure awareness training and other educational tools designed to build knowledge of security are tailored to the needs and learning styles of the individual

TIPS FOR POSITIVELY INFLUENCING COMMUNICATION

1. Resonate with your audience.
    a. Whether you are addressing senior management or front-line staff, the information must be provided in a way that is digestible and relevant to them.
    b. Listen to their concerns.
    c. Find out what is important to them and why.
    d. When explaining why certain security measures are important, be sure to communicate why they are important for them, for example, explain how the measure will affect their work, how will they benefit, and what impact it will have on them.
    e. Speak using language that resonates with your target audience.
2. Keep members informed.
    a. Attitudes towards security measures are more likely to be built positively if members understand the necessity of the various steps that are made to secure the organization and its assets.
    b. Share what steps are being taken, why they're important, and what impact they will have (on the business as a whole, and on them individually).
3. Encourage positive expression.
    a. The more often an attitude is expressed the stronger it becomes (see Attitudes), whereas an attitude that is not expressed frequently is likely to be weakly held.
    b. Build a network of security ambassadors across different business areas.
    c. Encourage and support security champions.

TIPS FOR POSITIVELY INFLUENCING COMPLIANCE

1. Improving the quality of communication channels to discuss security-related issues and report incidents (See Communication)
2. Increasing the understanding, knowledge and awareness of the policies themselves, including procedures to implement them into daily work tasks and activities (See Cognition)
3. Strengthening the understanding of how important their role is as a critical factor in sustaining or endangering the security of the organization (See Responsibilities)
4. Supporting the attitudes towards the importance of security (See Attitudes)

TIPS FOR POSITIVELY INFLUENCING NORMS

Positive norms that support organizational security are internalized when employees' values and behaviours are aligned with those expected. Behaviours that are supportive of organizational security need to be identified taught and reinforced (See Behaviours). When correct and expected behaviours are accepted as normal, adherence to these norms can be encouraged through the following mechanisms:

1. Expectations can be set through information security policies and role responsibilities. When desired actions are communicated and accepted by the group, they help consolidate policies into normatively acceptable behaviour (See Responsibilities).
2. Design campaigns that advertise information security-related social norms. Encourage employees to share their stories using blogs, newsletters, e-mails, etc, so that others become aware of the consequences of non-compliance and see others rewarded for adherence to norms (See Communication).
3. Internal communication channels should be open and accessible to address any uncertainty and share best practices. Sharing lessons learnt, celebrating achievements, exemplifying correct behaviours, and acknowledging concerns are all proven mechanisms (See Attitudes).
4. In addition, the role of organizational punishment can be considered a form of social control. When used as a legitimate deterrent, punishment facilitates the distinction between desirable and undesirable acts and helps to establish group norms by identifying acceptable and unacceptable behaviours.

TIPS FOR POSITIVELY INFLUENCING RESPONSIBILITIES

In any organization, security is everyone's responsibility. How people understand that responsibility is a key component of security culture. To improve, we offer the following advice:

1. All members must understand that they are all a part of the security system, even if they are not working on sensitive material. This knowledge and understanding will make every member less likely to put the organization in danger through risky actions (See Compliance).
2. Managers should make sure all members of their teams understand how the security system is a vital part of the organization and how they are all connected and responsible for securing their assets by acting responsibly and following the right procedures (See Norms).
3. Time should be taken to explain to every member of the organization how they fit into the security system of the organization. Because, when everyone is aware of their place within the organization's security, each person can more easily see how they can improve the security situation through their actions (See Cognition).
4. Managers should talk with the members of their teams regarding their responsibilities and how they can improve the security culture of the team and organization. Furthermore, managers should encourage dialogue between themselves, team

members and security officers, to further knowledge of the responsibility they all have for the security situation of the organization. (See Communication).

APPENDIX B: SUGGESTED BEST PRACTICES FOR BUILDING A CYBERSECURITY CULTURE

These suggestions related to best practices for building cybersecurity culture are given by Huang & Pearlson (2019):

occasional emails warning about suspicious behavior
seminars; mandatory training; treasure hunts; games
Report if there is bug over SLA, Security policy violations
Regular explicit training, external red-teaming, all-hands presentations, ubiquitous discussion in culture, separate internal- and external-facing email systems.
online self test required yearly
Internal SpearPhishing Exercises
We treat employees as "sensors" who are encouraged to detect and report cyber events. We are responsible and held accountable for patching our own systems.
Training, fake phishing emails
E-Mails to test employees on accessing
I give lots of internal talks, both on specific ways we can improve, but also on technologies and general problems in the space.
Security Awareness Training monthly, Simulated phishing tests, posters, newsletters
Yearly training
Training and table top simulation exercises
Security awareness videos
Biometric Authentication on the Blockchain
Annual training requirement for all employees; quarterly "fake phishing" exercises to test employees; bi-annual discussion at Corporate Town Halls; 8-12 articles annually disusing recent incidents and best practices on company intranet; proprietary software looking for improper downloads and/or IP addresses that are not typically used/
mandatory cyber security awareness training, phishing simulaitons
Regular phishing exercises for training
Employee education. Tech solutions are good, but education is best
New it-strategy with principals for cyber security
Regular password changes, approved company-wide shared cloud platform, limited access to web services,
periodic mandatory training in cybersecurity practices and insider threat
Security (Cyber) Strategic Plan & Roadmap mapped to the Customer Experience Strategy; Reward & Recognition on Cyber Practices; Lunch & Learn including industry experts on data, privacy, law enforcement; Change Management Program on Best Practices to Security and Cyber.
Mandatory for new employees to sign a User Agreement including an Acceptable Use and Cyber Security Policy. It's never followed up on though. There was a cyber threat briefing held by the CISO a few years ago that every employee had to attend, ordered by the board after a major cyber incident. But it was an one-off effort and nothing similar has been done since. Top priority is focus on the core business and cyber security is not a main concern.
LastPass and Yubikey send-factor used by all employees both for work and personal use.All cybersecurity vulnerability scanning tools, configuration management and release mechanisms, etc. are built with 100% free and open source (FOSS) software. Bringing modern cybersecurity practices to US Federal agencies (DoD, HHS, DoED, etc.) is difficult as they want FISMA compliance with 3-year ATO schedule, which is far from appropriate to manage today's threat landscape. But getting an AO to look at (e.g.) GitHub or Graylog dashboards can be surprisingly difficult, as MS Word documents are more within their comfort zone.
Phishing testing, currently annual awareness training. Beginning stages of ISO 27001 certification at customers request, security was not a priority prior to this request.
Basic Security & Privacy Awareness eLearning Module; Phishing Awareness Exercises
"Don't Feed the Phish"-Mandatory on line training to educate company about how to avoid phishing attacks. Compliance was formally tracked throughout business. Also have annual mandatory online training on general security matters
third party contract, next generation firewall contract
Cybersecurity training for all new hires
Implemented IT Security Policy
ISO 27001:2013 implementation and certification
Annual training and frequent email notices.
RMF audit
if you lost your laptop - you lose your job
Beginning work on creating policies and procedures and incident reporting.
Getting rid of an ineffective CISO and bringing in a new CISO
KnowBe4 user training and simulated tests have been effective
Mandatory training, active infosec dept, sysdev and sysops training, publicizing incidents and MO of perpetrators, etc
Security discussed at weekly business meeting
randomly times social engineering testing
Our managed desktops use screensavers with various cyber security best practices
Interest was brief after a breach of employee personal data. It quickly faded.
annual awareness Training
Annual on-line training
Awareness training, and rewarding good behavior.
sec awareness, data protection policy
Awareness sessions
training, phishing campaigns
Phising simulations
KnowBe4 monthly training / quarterly phishing
MFA
Timely, and relevant security awareness training.
Training sessions, marking EXTERNAL on messages from outside the organization
security awareness training; phishing campaign; intranet bulletins;
limited training, phishing awareness campaigns, screen saver messages.

APPENDIX C: QUALITATIVE SURVEY QUESTIONS

THE QUALITATIVE SURVEY QUESTIONS BY PARTICIPANTS

QUESTIONS FOR STUDENTS

Q1: How do you feel while using modern technology?

Q2: How much aware are you regarding possible cyber-attacks and resultant damages?

Q3: Do you regularly update your digital devices?

Q4: How would you describe your cybersecurity knowledge? Please briefly describe your familiarity with the basic cybersecurity principles or practice in terms of awareness, training or education.

Q5: Are you happy with the current cybersecurity state at your institution (e.g. the practice of frequently changing passwords, not using college's computers for personal purposes)? Please briefly describe.

Q6: How familiar are you with the cybersecurity practice at the college? Please briefly describe.

Q7: Do you adhere to the prescribed cybersecurity practice at the college (e.g. not open unknown attachments or follow the link to an unfamiliar website)? If yes, please briefly describe.

Q8: How often do you visit unfamiliar websites by clicking on the link in an email?

Q9: While receiving an email containing a suspicious link would you:

- Carry on by clicking the link and enjoying the website content?
- Ignore that email and not visit a potentially interesting website?
- Report that email and ignore the suspicious link?

Q10: Somebody recommended to you a website with exciting content but unfamiliar to you. Would you:

- Encourage your peers, relatives or family to visit potentially interesting websites even if are not familiar with potential damages caused by that action?
- Caution them that website might be dangerous?
- Ignore the recommendation?

Q11: Do you know to whom to report a cyber incident that happened to you? Please describe briefly.

Q12: How familiar are you with the college's cybersecurity policies?

Q13: How familiar are you with the college's general culture (e.g. acceptable and unacceptable behaviour)?

Q14: How aware are you of cybersecurity risks for you and the college while using ICT devices (e.g. PCs, tablets, smartphones)?

Q15: How much do others influence your behaviour while using ICT devices at the college or in the online interaction with the college? Please describe briefly.

Q16: How much the environment influences your behaviour while using ICT devices at college or in the online interaction with the college? Please describe briefly.

QUESTIONS FOR TEACHERS ONLY

Q1: How would you describe your cybersecurity knowledge? Please briefly describe your familiarity with the basic cybersecurity principles or practice in terms of awareness, training or education

Q2: How would you describe your knowledge understanding and awareness of cybersecurity issues?

Q3: How familiar are you with the college's cybersecurity policies?

Q4: What would be a benefit for teachers and students from attending cybersecurity awareness programmes?

Q5: Is there a syllabus dedicated to cybersecurity or cybersecurity culture? Please describe briefly.

Q6: What would be a benefit for students from a cybersecurity syllabus? Briefly describe the usefulness of cybersecurity training programme/s.

Q7: How familiar are you with the college's general culture (e.g. acceptable and unacceptable behaviour)?

Q8: How much is currently cybersecurity culture integrated into the college's general culture? Please briefly describe.

Q9: How cybersecurity syllabus and awareness campaigns are or should be delivered (e.g. online, offline, combined)? Please describe briefly.

QUESTIONS FOR TEACHERS AND MANAGEMENT

Q1: Who is responsible for cybersecurity at the college (e.g. certain departments, management, teachers, everybody)?

Q2: What is the state of the cybersecurity communication at the college (e.g. quality, frequency, communication channels: email, posters, etc.)?

Q3: Compliance refers to knowledge of written cybersecurity policies and the extent that people follow them. How familiar are you with the college's cybersecurity policies, rules and procedures?

Q4: How familiar are you with the college's cybersecurity norms (e.g. terms of use of the college's ICT equipment)?

Q5: Do you know to whom to report a cyber incident that happened to you? Please describe briefly.

Q6: How do you perceive your role in cybersecurity while at the college?

Q7: How do you view cybersecurity at the college (e.g. as an integral part of teaching and learning, separate issue)? Please describe briefly.

Q8: How satisfactory is the college's management involvement in cybersecurity at the institution (e.g. active participation, championing, financing)?

Q9: How training programs and cybersecurity policies are available at the college?

Q10: How familiar are you with the college's cybersecurity policies?

Q11: How well are cybersecurity roles of the stakeholders at the college defined (e.g. senior managers, IT people, human resources, legal department, teachers, students)?

Q12: In what way general national environment and happenings influence your behaviour related to the use of ICT at college or in the online interaction with the college?

Q13: To what extent are you familiar with the cybersecurity strategy? Please describe briefly.

Q14: How effectively is the college's cybersecurity strategy is implemented?

Q15: How often is conducted cybersecurity training or cybersecurity awareness campaigns? Please describe briefly.

Q16: How has cybersecurity culture been measured thus far? Please describe briefly.

THE QUALITATIVE SURVEY QUESTIONS BY THEMES

ATTITUDES

Affective

Q1: Are you happy with the current cybersecurity state at your institution (e.g. the practice of frequently changing passwords, not using college computers for personal purposes, not using personal devices for teaching or learning purposes)? Please briefly describe.

Cognitive

Q1: How familiar are you with the cybersecurity practice at the college?

Behaviour

Q1: Do you adhere to the prescribed cybersecurity practice at the college (e.g. not opening unknown attachments or following the link to an unfamiliar website)?

COGNITION

Q1: How would you describe your knowledge understanding and awareness of cybersecurity issues?

Q2: What would be a benefit for teachers and students from attending cybersecurity awareness programmes?

Q3: What would be a benefit for students from a cybersecurity syllabus?

COMMUNICATION

Q1: What is the state of the cybersecurity communication at the college (e.g. quality, frequency, communication channels: email, posters, etc.)?

COMPLIANCE

Compliance refers to knowledge of written cybersecurity policies and the extent that people follow them.

Q1: How familiar are you with the college's cybersecurity policies, rules and procedures?

NORMS

Q1: How familiar are you with the college's cybersecurity norms (e.g. terms of use of the college's ICT equipment)?

RESPONSIBILITIES

Q1: Do you know to whom to report a cyber incident that happened to you? Please describe briefly.

Q2: How do you perceive your role in cybersecurity while at the college?

LAYERS OF CYBERSECURITY CULTURE

Tactic assumptions

Q1: How do you view cybersecurity at the college (e.g. as an integral part of teaching and learning, a separate issue)? Please describe briefly.

Espoused values

Q1: Who is responsible for cybersecurity at the college (e.g. certain departments, management, teachers, everybody)?

Artefacts

Q1: How satisfactory is the college's management involvement in cybersecurity at the institution (e.g. active participation, championing, financing)?

FACTOR IMPACTING CYBERSECURITY CULTURE

Q1: How familiar are you with the college's general culture (e.g. acceptable and unacceptable behaviour)?

Q2: How much is currently cybersecurity culture integrated into the college's general culture?

The roles to be played by different stakeholders groups

Q1: How well are cybersecurity roles of the stakeholders at the college defined (e.g. senior managers, IT people, human resources, legal department, teachers, students)?

Human factors in cybersecurity culture

Q1: How aware are you of cybersecurity risks for you and the college while using ICT devices (e.g. PCs, tablets, smartphones)?

Q2: How much do others influence your behaviour while using ICT devices at the college or in the online interaction with the college? Please describe briefly.

Q3: How much the environment influences your behaviour while using ICT devices at college or in the online interaction with the college? Please describe briefly.

Q4: In what way general national environment and happenings influence your behaviour related to the use of ICT at college or in the online interaction with the college?

CYBERSECURITY CULTURE STRATEGY

Q1: To what extent are you familiar with the cybersecurity strategy? Please describe briefly.

Q2: How effectively is the college's cybersecurity strategy is implemented?

IMPROVING CYBERSECURITY CULTURE THROUGH EDUCATION

Q1: Is there a syllabus dedicated to cybersecurity or cybersecurity culture? Please describe briefly.

Q2: How often is conducted cybersecurity training or cybersecurity awareness campaigns? Please describe briefly.

FORMS OF DELIVERY CYBERSECURITY CULTURE PROGRAMMES

Q1: How cybersecurity syllabus and awareness campaigns are delivered (e.g. online, offline, combined)? Please describe briefly.

MEASURING CYBERSECURITY CULTURE PROGRAMMES

Q1: How has cybersecurity culture been measured thus far? Please describe briefly.

APPENDIX D: CURRICULUM PRACTICAL TOPICS

SECURITY MEASURES IN THE DIGITAL ENVIRONMENTS DOMAIN

These topics are suggested by Civilcharran (2020)

Digital Content Security Skills

a) The ability to delete sensitive digital content by using third-party wiping tools to avoid hackers from accessing sensitive digital content from the digital trashcan and run a tool such as PANscan to confirm that sensitive digital content has been correctly deleted.

b) The ability to maintain secure user IDs and passwords by complying with password policies and guidelines to ensure that the password is strong enough to prevent unauthorised access to email accounts, websites and computer systems.

c) The ability to protect digital content against accidental damage by applying guidelines on preventing accidental damage, especially those guidelines relating to accidental damage that is not covered by insurance policies.

d) The ability to protect the unauthorized use and modification of digital content by authentication, content protection, as well as implementing access rights and availability.

e) The ability to comply with legal issues regarding digital content by being knowledgeable of the various legal issues of social media, copyright laws and consequences of non-compliance.

f) The ability to determine the trustworthiness of digital sources by evaluation of the author, date, other sources citing a digital source, web domain, the accuracy of the source, writing style and the design of the website.

g) The ability to identify digital frauds, suspicious activity and cyber-crimes by understanding the types and causes of cyber-crimes and digital fraud that exist.

High-Level Technical Security Skills

a) The ability to use anti-virus software to protect against a cyber-attack by ensuring that virus definitions are regularly updated and frequent virus scans are performed, manually or automatically.

b) The ability to install a local firewall on computer devices to control the outgoing and incoming network traffic to prevent malware from spreading across the network.

c) The ability to securely send and open digital messages and content by using digital certificates, digital signatures, and other security tools that support this digital skill.

d) The ability to securely connect to networks by encrypting important files and folders, using the HTTPS web address[20], connecting to trusted networks, disconnecting from a network once complete, running a Virtual Private Network (VPN), and being cautious of shoulder surfing[21] when entering passwords.

e) The ability to encrypt sensitive information stored on a device by using full-disk encryption to encrypt all data on a device, for example, BitLocker for Windows and FileVault for MacOS.

f) The ability to back up and store digital content on a local computer network or network drive by scheduling incremental backups and setting up the synchronisation service.

g) The ability to back up and store digital content on the Cloud, such as Google Drive and DropBox by performing incremental backups and setting up the synchronisation service.

Personal IT Security Skills

a) The ability to practise safe online behaviour by limiting personal information, practising safe browsing, enabling privacy settings, using a secure Internet connection, downloading from trusted sources, using strong passwords, purchasing from secure websites, ensuring antivirus is up-to-date, being cautious about what one posts, and by being wary about who you meet online (Kaspersky, 2020).

b) The ability to secure personal information against identity threats by understanding the threats of distributing personal information and following guidelines, such as using updated security software, identifying spam and scams, and monitoring bank statements to protect against threats.

c) The ability to maintain a secure digital footprint[22] by following guidelines, such as reviewing mobile usage, regularly updating software, using strong passwords, checking privacy settings, building one's reputation, and checking which sites have personal information that needs to be removed (NortonLifeLock, 2020).

d) The ability to report suspicious online activity by understanding what constitutes 'suspicious online activity, and obeying policies and procedures regarding the reporting of suspicious online activity, to prevent cyber-attacks and other fraudulent activities.

e) The ability to report breaches in security by understanding and complying with the organisational or national rules and regulations of reporting breaches, and the risks of non-compliance.

f) The ability to comply with the employer's digital policy by understanding the policy and the legal implications of non-compliance.

APPENDIX E: ACTION RESEARCH AND CASE STUDY IN CYBERSECURITY RESEARCH

CASE STUDY

A Case Study is a well-established research method that is characterized by analysing cases (i.e., a bounded system) as the units of analysis. Cases can be certain events, projects, people etc. Depending on the number of studied cases and their interdependence, case studies can follow various case study designs, such as single-case and multiple-case studies (Brantlinger, et al., 2005). Case studies are an observational research method that systematically combines various types and sources of data in a rigorous data analysis process (Bennett & Elman, 2006; Colicchia et al., 2019).

To achieve an adequate level of credibility, various forms of triangulation are commonly applied in case studies (e.g., data triangulation, method triangulation, and researcher triangulation) (Bennett & Elman, 20062; Yin, 2017).

Using quantitative (e.g., survey) data is nothing unusual in case studies. However, case studies may achieve their interpretive and descriptive richness only after confronting both quantitative and qualitative data (Parry et al., 2014; Yin, 2017).

Despite the common misconception that case studies may only be good for exploratory studies and theory building, case studies can be used for all theoretical purposes (i.e., theory generation, elaboration and testing) (Colicchia et al., 2019; Parry et al., 2014; Yin, 2017].

For example, case studies may complement the knowledge of statistical correlations determined by quantitative research methods by providing in-depth insight into whether the hypothesized underlying mechanisms are indeed working as expected and why (Fujs et al., 2019).

ACTION RESEARCH

Action research is about implementing ideas in practice while collecting data at the same time. Unlike other quantitative methods, it is designed for the research to influence the research settings by providing ideas and implementing them in practice (Brantlinger, et al., 2005).

In addition to pure action research which is guided only by the researchers, collaborative or participatory action research also exists (Brantlinger, et al., 2005; Fletcher & Marchildon, 2014; Schneider, 2012).