Kalpa Publications in Computing

Volume 12, 2019, Pages 202–212

Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems 2019

Challenges in Information and Cybersecurity program offering at Higher Education Institutions

Seapei Nozimbali Mogoane[1] and Salah Kabanda[2]

University of Cape Town, Department of Information Systems
sea.mbali@gmail.com[1], salah.kabanda@uct.ac.za[2]

Abstract

This study examines the role of higher education institutions (HEIs) in addressing cybersecurity challenges, in the wake of a prominent shortage of skills, specifically those related to information and cybersecurity professionals. Using qualitative semi structured interviews, the study sought to identify the factors influencing the offering of an information and cybersecurity curriculum at HEIs. The findings show that internal influencing factors were top management and individual academic's awareness of information and cybersecurity, internal expertise, offering the program only at postgraduate level, and the workload and bureaucracy associated with having the program. External factors perceived to influence information and cybersecurity curriculum at HEIs include pressure from industry and stakeholders as well as institutional bodies that help shape curriculum development.

1 Introduction

Information systems and technologies has transformed human habitation and life in general. Technology is now regarded an essential commodity that impacts our economies, social and governmental necessities (National Academics of Science Engineering Medicine, 2018). One of the important debates in academia has been how to secure these systems, specifically against the ever ongoing and evolving cybersecurity vulnerabilities. For example, given that a nations critical infrastructural component is comprised of, amongst others, healthcare, energy distribution, transportation, governmental operations, and financial services; it becomes important to secure the information used, handled and managed by these institutions. Furthermore, the effective functioning of these sectors and their ability to provide services to communities and global organizations, depends on the flow of reliable data, of which integrity should be maintained, availability ensured, and

confidentiality protected (Kessler and Ramsay, 2014). To this end, information security becomes important, since "information is the asset that has to be secured" (Von Solms and Van Niekerk, 2013).

Yet, IT systems are consistently under great threats, attributable to human nature mistakes, malicious and immoral activities. The need to address this problem has never been more calling in this era of information and cybersecurity; and in an environment that falls short of qualified professionals (Rowe et al 2011). Whilst the shortage of professionals is a worldwide phenomenon, this challenge is more worrying for emerging countries which have to also face contextual challenges such as resource allocation towards curbing information and cybersecurity, poor security hygiene and piracy (Ben-David et al, 2011). This study examines the role of higher education institutions (HEIs) in addressing cybersecurity challenges, in the wake of a prominent shortage of skills, specifically those related to information and cybersecurity professionals (Parker and Brown, 2018). The objective is to identify the factors influencing the offering of an information and cybersecurity curriculum at HEIs.

This study is contextually placed in South Africa where there has been reports of an increase in hacktivism and number of information and cybersecurity incidents caused by accidental/misconfiguration perpetration (Van Niekerk, 2017). The rest of the study is arranged as follows: Section 2 presents the related work on information and cybersecurity. Section 3 outlines the method and techniques employed to carry out the study. Section 4 presents the findings and Section 5 concludes the study.

2 RELATED WORK

2.1 Information and Cybersecurity

The increase in the use of IT systems in our everyday lives has made individuals and business alike become more vulnerable to cyber-attacks that disrupt a computer's normal operations and sensitive information loss through malicious network attacks (Ben-Asher and Gonzalez, 2015). This has implications on the information as well as the individual or organization with the information. Von Solms and Van Niekerk (2013) sees cybersecurity as the protection of information resources (information security), together with other assets, including the person him/herself. They clarify that whilst in information security, the human element refers to the role of humans in the information security environment and processes; in cybersecurity context, humans are potential targets of cyber-attacks knowingly or unknowingly (97). It therefore becomes important to safeguard measures in place to protect information and the human factor dimension. However, this is proving difficult due to the quick pace of technological innovations and most importantly due to the "intentional community effort" required from academia, industry, government, and public participation (Paulsen et al, 2012).

Whilst the interplay and engagement of these four community efforts (academia, industry, government, and public participation) is important, this study focuses on the role of academia in addressing information and cybersecurity, mainly because of the lack of information and cybersecurity professionals whose core function is to protect organizations from cybercrime and other cyber related threats (Parker and Brown, 2018); and most importantly because "the academic, skills and training fraternity do not merge strategies and actions that would be acceptable for industry and governmental sectors in a harmonized fashion" (Dodge et al, 2012). A call has been made for cybersecurity educators and trainers to pay attention to "the lack of youth joining the profession, the insufficient exposure to information and cybersecurity concepts, the absence of established career and training pathways into the profession, and the shortage of suitably qualified teachers" (National Cyber Security Strategy, 2016). According to Rowe et al (2011), there is currently a shortage of approximately 20 000 to 30 000 qualified information security professionals in the US public sector despite the fact that the field is

one of the best compensating fields. Even with the existing cybersecurity workforce, Dodge et al (2012) notes that they are "lacking in meeting information technology societal demands" and this is partly because current cybersecurity skills and competencies tend to be limited to IT personnel, whilst general employees are given general awareness and education programs that are insufficient to address the ongoing cyber-attacks (Adams and Makramalla, 2015; Kessler and Ramsay,2014). The ITU National Cybersecurity Strategy Guide (2011) identifies capacity building as one of the main pillars of global cybersecurity agenda and cites a skilled cybersecurity workforce as a necessity for any nations. ITU identifies three key strategic areas to facilitate cybersecurity human and institutional capacity building as shown in Figure 1.

Management	Information Assurance	Technical
• Cybersecurity Strategy • Legal and Regulatory • Cybersecurity business case formulation • IT Base skills • Staff Management skills/ Leadership skills • Personnel Security • Multi-Disciplinary skills (technology, people etc) • Communication skills • Cyber-Criminal Psychology • Cyber-Ethics Skills	• Cybersecurity Policies, Standards and Procedures • Risk Management • System Accreditation • Compliance Checking • Audit and Monitoring • User Rights and Responsibilities • Incident Management Process Design • Assurance, trust and confidence mechanisms	• IT technical skills (security management) • IT technical skills (Security deployment) • Security Design Principles e.g. zoning • Resilient Infrastructure • Data Protection/ System administration • Cryptographic and Applied Crypto Skills • Data custodianship • Operational Security • Incident Management

Fig. 1. Typical Cyber Security Skills (ITU 2011)

The three strategic areas, Management, Information Assurance and Technical Capabilities coupled with their typical required skills in Fig.1. are grouped to provide direction for countries with shortage information and cyber security workforce (ITU 2011). Kessler and Ramsey (2014) propose a cybersecurity program comprised of six courses – see Figure 2 below.

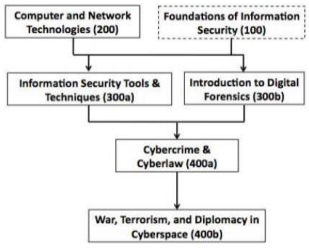

Fig. 2. Proposed cybersecurity six courses (Kessler and Ramsay, 2014)

The first course is the Foundations of Information Security which seeks to address "operations, governance, applications, purposes, and strengths and limitations to information assurance and incident response activities". Then is the Computer and Network Technologies course which exposes students to communication networks. At third year, students are given hands-on and introduced to proactive offense and defense tools via the Information Security Tools and Techniques course, as well as tools and techniques of reactive offense and defense via the Introduction to Digital Forensics course. Then, at fourth year, students become exposed to Cybercrime and Cyberlaw, a course whose intent is to address criminal behavior in, and evolving laws governing cyberspace. Finally, a course on War, Diplomacy, and Terrorism in Cyberspace is presented to allow the exposure to the current era of cyberterrorism and cyberwarfare.

Most cybersecurity curriculums are grounded in the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework) which prepares, and provides

knowledge and skill sets that are comprehensive in nature covering legal, managerial and social aspects on information and cyber security. Such a curriculum, therefore should be cognizant of the "optional courses, within and outside the traditional computer science, computer engineering, information systems management, or information assurance topic areas" (77). The NICE Framework is a "reference structure that describes the interdisciplinary nature of the cybersecurity work and sharing information about cybersecurity work and the skills (KSAs) needed to complete tasks that can strengthen the cybersecurity posture of an organization" (Newhouse et al 2017). The framework consists of seven categories, and under each category are specialty areas, which are then followed by relevant KSAs. The seven categories are reflected in the figure below

Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Fig.3. Seven NICE Framework Workforce Categories (Newhouse et al 2017)

2.2 Cybersecurity in developing countries

Manson and Pike (2014) argue that the NICE Framework is a useful framework but "mastering KSAs requires ample time, measured in hours of relevant practice and performance measurement". They call educators and trainers to address the depth in cybersecurity education, given the increasing need and shortage of such skill sets. This call is particularly important for developing nations that have very little cybersecurity initiatives despite having "the fastest growth in internet users" (Muller, 2015) and "where a dependence on technology or use of technology infrastructure to support applications such as E-Government, E-Commerce means that cybersecurity issues require investigation" (Cole et al 2008). Dlamini et al (2011) observed that the African continent is collectively vulnerable with regards to cybersecurity and went to propose a framework "for an African cybersecurity policy which addresses specific country related governance, information and cybersecurity awareness and training, management of incidents, research and development that is global oriented" (29). They also propose a framework that promote information and cyber security resilience to inform African policy development. South Africa is one of the few countries on the African continent with a national cybersecurity policy framework to address the cybersecurity environment. Yet, despite these policies, there remains minimal awareness of and information and cybersecurity professionals. It is therefore imperative to understand the factors influencing the development and offering of information and cybersecurity curriculum at higher education institutions in South Africa.

3 METHODOLOGY

To identify and understand the factors that influence how higher education institution (HEIs) develop and offer information and cybersecurity curriculum, this study followed a qualitative approach. The study was inductive in nature, requiring participants to engage with the phenomenon of interest - information and cybersecurity curriculum development. Six participants from four Higher Education Institutions (HEIs) agreed to participate in the study as shown in Table 1.

Participant	Higher education Institution	Position
Uni_A	University A	Senior Lecturer (PhD)
Uni_{B1}	University B	Head of school of IT and Computer science
Uni_{B2}	University B	Lecturer (PhD)
Uni_C	University C	Lecturer (PhD)
Uni_{D1}	University D	Lecturer (PhD)
Uni_{D2}	University D	Lecturer (Masters)& Extensive industry experience

Table 1. Six participants from Higher Education Institutions (HEIs)

Data was collected using semi structured interviews to explain the factors influencing curriculum development. Further, archival data on policies and related regulatory frameworks on information and cybersecurity was included.

The population was the South African HEIs and the sample size was specific to HEIs that offered technology driven courses such as information systems or computer science in their mainstream qualification. Whilst we recognize this as a limitation, it is a starting point in determining the influencing factors associated with a curriculum offering in information and cybersecurity. Collected data was thematically analyzed to identify and organize the data to allow the derivation of meaning and themes. Seven themes emerged which are discussed in the next section.

4 FINDINGS

4.1 Awareness of Information and Cybersecurity

Findings reflect that most South African HEIs were aware of information and cybersecurity and its evolving nature. According to participant Uni_A:

> *the emphasis before was on computer security. Now we have information security. Information security is required because, we don't just want to secure the physical computer and what it interacts with anymore. We also need to secure the information that's used on there as well.*

The shift towards information security was perceived to be important and according to Uni_C: *the safe guards we put in place to protect information cannot be undermined or compromised.* Participant Uni_{B2} was of the opinion that information security was not a new concept:

it started many years ago, it was mostly focused on security and protection of information and information systems inside a company. That means it was protecting unauthorised access, you had to use disclosures, disruptions and modifications within the company with the aim to promote confidentiality, integrity and availability but most of that was always inside a company. If you look at cybersecurity, I see cyber security as a super subset of information security, because cyber security is much more country wide, networks and international.

Although these participants appeared to be aware of cybersecurity, participant Uni_{D1} was of the view that: *awareness at this level alone is not sufficient. We need our leaders to be aware and act. Most of them do not understand the implications posed by cybersecurity, and that is the problem*. These findings are consistent with prior studies which indicated that in developing countries, "there is a lack of training and awareness among the employees and computer users" (Choejey et al, 2015). Awareness was therefore perceived as a prerequisite for "taking action" and lack of awareness at management level was a barrier towards offering information and cybersecurity program. These empirical findings confirm those from the archival data that there was "limited awareness from the public and businesses" in matters of cybersecurity (Department of Telecommunications and Postal Services, 2017); and reaffirms the need for management to be considered in information and cybersecurity management (Soomro et al 2016).

4.2 Lack of program offering at undergraduate

There was a general perception that HEIs are lagging behind in the introduction and offering of information and cybersecurity studies. All participants noted that the program is offered at postgraduate level - specifically at the master's level. This was perceived as a challenge because some students at postgraduate level did not have the fundamental background required to engage with the key issues in information and cybersecurity at postgraduate level as participant Uni_A indicates:

this year - it's the first time that we are doing it (teaching cyber and information security courses) at our university in information systems and we are teaching it at the honours level. So, any form of cyber and information security specialization is only at honours level and master's as well as computer science which has a master's in computer security. I have introduced them to firewalls and VPN but I haven't done those in detail because they don't have the undergraduate technical background and experience. I have only had time to really explore the threat modelling and I have done some of the controls.

These findings show that despite having an information security/cyber security program offered at postgraduate level, the program lacks depth due to the lack of preparedness of the incoming students, thereby calling for the program to be offered at undergraduate level. These findings echo Avery and Oakley (2019) who "argue that the current IS programs are providing insufficient security training through modules which do not provide a sufficient amount of detail on IT security as required in the current technological environment and through separate elective IT security course". We also observe that whilst some HEIs in developed economies are attempting to introduce cybersecurity as a primary academic discipline in addition to their current offering of cybersecurity at their undergraduate degrees in traditional disciplines such as computer science (Gibson et al 2019); developing countries are still lagging behind, thereby failing to provide students who would then become new entrants into the market with awareness of and understanding of information and cybersecurity.

4.3 Limited availability of Information Security skill sets in HEIs

Some participants were of the view that the development and the offering of an information security curriculum was challenging in comparison to other information systems courses. Participant Uni_{D1} attributed this to the *lack of professionals. We simply don't have them and even if we have them, the industry offers them quite a lot in terms of salary. Competition is tough out there*.

Participant Uni_A agreed citing that information and cybersecurity are:

new offerings on the market and the skill sets are limited from the academic practitioner point of view. I had to ask two professors to look at my module outline first before I developed it further and they both are information security experts, that's their research area.

This participant was of the view that having two information security specialists in their department is a bonus because *in some institutions they have none*. Given that this participant is from an affluent HEIs which is relatively well resourced, highlights further the problem in developing countries of "having access to and adequate cybersecurity professionals with adequate motivation and skills to prevent, detect, respond, or even mitigate the effect of such threats" (Mouheb et al 2019).

4.4 Multidisciplinary nature of Information and Cybersecurity

The lack of specialist was not perceived as the only challenge. Another was the multidisciplinary nature of the concept of security and a perception that there was a lack of integration of ethics and legal studies into the curriculum. Participant Uni_{B2} explained that teaching student's issues of information and cybersecurity requires the program to be comprehensive enough to allow for multidisciplinary participation; *but unfortunately, the legal aspects and ethics were only mentioned but not really covered*. Participant Uni_{D2} was of the opinion that:

cybersecurity should not be seen as belonging to one department. Once we do that, we box everything about it, including how we teach it – from one or two departments and that's us [Information Systems] or computer science.

Due to this shortcoming, which was also experienced at other institutions, $Uni_{A:}$ *made them [students] do research on their own on digital forensics to make them aware of the legal issues surrounding cybersecurity….and that's the global way of looking at it.* In order to sensitize students on issues of security, $Uni_{C:}$ *included a component in the final year project, to ensure that the system developed is legal in the sense that it complies with accounting practices and conforms to user's privacy.*

The legal and regulatory challenge has also been expressed by the South African Department of Communications [(2010), that:

there were many legal provisions addressing information and cybersecurity in South Africa. However, these provisions did not adequately address the legal challenges South Africa faces to effectively deal with cybercrime.

These findings reaffirm Ruiz's (2019) position that cybersecurity courses need to be transformed towards a multidisciplinary direction that involves "a multi-stakeholder platform that unites industry, government and academia to actively address national information and cybersecurity educational requirements and strategies is urgently required." (Catota et al, 2019).

4.5 Workload associated with program development

All participants identified the lack of time to invest in the development of a good program offering; and the bureaucracy involved to have the program recognised. So, whilst participants recognized the importance of the program, having the program recognized by going through the relevant accreditation bodies was a challenge as Uni_{B1} explains:

Having the program ready is one challenge. The next part is to offer SAQA [The South African Qualifications Authority] and HED [Higher Education Department] forms that you have to fill in to get it registered on the system and the forms that you applied to do the courses is very cumbersome it must go through a lot of committees, external evaluators and things like that can take like between two to three years, from the start to implementation.

These findings imply that bureaucracy is heightened when developing and embarking on the accreditation of an information and cybersecurity program than other programs due to the multi-disciplinary nature of the program and having diverse number of stakeholders involved in the development of an information and cybersecurity program. Similar findings are reported by (Catota et al 2019) who posits that bureaucracy and over-regulation at HEIs in developing countries and the lack of university autonomy makes "implementing an information and cybersecurity program at the undergrad level tough and burdensome".

4.6 Information and Cyber Security Institutional bodies

Consultation with the institutional bodies for information and cybersecurity was perceived as important for all participants. Specific bodies included the International Federation for Information Processing (IFIP) conference specializing in information security and privacy. Several institutional bodies assisted the development of the curriculum at each institution. For example, Uni_{D2} reports that:

> *we are part of the Association Computing Machinery network and so we get most of the latest information there, we also have invited scholars in this area of research and they help to shape our work and curriculum development*.

Participant Uni_{D1} adds that some academics are *engaged with industrial and government projects which then feeds into our research*. According to this participant, using cybersecurity knowledge to solve industrial and local problems was rewarding, although challenging due to the *confidentiality and bureaucracy* involved. Participant Uni_A consulted the *IFIP Cybersecurity curriculum to guide the process of curriculum development*. According to participant Uni_C their *curriculum is heavily influenced by the requirements of ABET accreditation, which dictates certain competencies that needs to be imparted to the students.*

The Accreditation Board for Engineering and Technology (ABET), provides accreditation as proof and confirmation that program has met standards crucial to produce graduates ready to enter the critical fields of STEM education (https://www.abet.org/about-abet/). Participant Uni_{B2}'s curriculum was influenced by:

> *key focus areas that we see important currently for us in the country. Initially, the curriculum came from the generic textbook on information security covering…which has been there for about eight to nine years it's a very old curriculum.*

None of the participants indicated the NICE framework or the ITU National Cybersecurity Guide in their narrative although it could be implicitly implied within the institutional bodies they consulted. For example, a report in the Computing Curricula Series Joint Task Force on Cybersecurity Education (2017) which IFIP is part of, uses the NICE Framework as a source. However, it was evident that the participants awareness of the NICE framework was limited.

4.7 Industry and Stakeholder Pressure

All participants identified the industry as one of the main pressure points towards the development of the information and cybersecurity program. According to Uni_A: *the industry partners are all saying we should have it [Information and Cybersecurity Studies], and that's why it's here now.* This is not surprising given that organizations are usually wearisome of any attack on their businesses and therefore they require the necessary skill sets from HEIs to address information and cybersecurity concerns.

However, according to the South African Department of Telecommunications and Postal Services (2017), only 37% of organizations have discussed an information and cybersecurity plan or strategy which still needs to be implemented, while 29% have a fully functional plan. This in itself is a concern. Additional pressure was from collaborating partners as Uni_B explained:

For our master's degree, we currently designing a curriculum with other universities in the country as part of the BRICS collaboration network and we want to do that qualification together with the other BRICS countries as well. We are learning along but it is a challenge to work at their pace.

The importance of partnerships has been highlighted by the South African Department of Communications in their cybersecurity draft policy (2010):

The development of interventions to address cybercrime requires a partnership between business, government and civil society. Unless these spheres of society work together, South Africa's efforts to achieve its cybersecurity policy objective will be severely compromised.

Previous studies have also called for industry stakeholders to participate in addressing the lack of cybersecurity professional (van Vuuren et al 2018).

5 CONCLUSION

The purpose of this study was to identify the factors influencing the decision to offer an information and cybersecurity curriculum at HEIs. The findings show that seven factors influence this decision. These seven factors consisted of internal and external factors. Internal factors specific to HEIs were top management and individual academic's awareness of information and cybersecurity; internal expertise, offering the program only at postgraduate level, and the workload and bureaucracy associated with having the program. External factors perceived to influence the decision to offer an information and cybersecurity curriculum at HEIs come from industry and stakeholders as well as institutional bodies that help shape curriculum development. Internal factors were perceived to be more influential as they paved the path to creating more awareness of information and cybersecurity and instrumental towards resource allocation. Understanding these internal and external factors is key as they shape how educators and institutional stakeholders develop the structure and contents (including the set of concepts, terms, and activities) that make up the information systems professional domain (Quezada-Sarmiento et al 2016).

Whilst the findings provide a better understanding of what influences HEIs to offer information and cybersecurity curriculum; the study has some limitations. The main limitation is the sample size which is small and this could be improved in future to offer more coverage. The sample size was small in this instance partly because participants specifically involved with teaching information and cybersecurity are currently few.

References

Adams, M., and Makramalla, M. (2015). Cybersecurity skills training: an attacker-centric gamified approach. *Technology Innovation Management Review*, 5(1), 5-14.

Association for Computing Machinery (2017). *Cybersecurity curricula*. Retrieved from https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Avery, A., and Oakley, R. L. (2019). The Business Case for IT Security as a Core Course in IS Curriculum. *Twenty-fifth Americas Conference on Information Systems*, Cancun, 2019

Ben-Asher, N., and Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, 48, 51-61.

Ben-David, Y., Hasan, S., Pal, J., Vallentin, M., Panjwani, S., Gutheim, P., and Brewer, E. A. (2011). Computing security in the developing world: A case for multidisciplinary research. In *Proceedings of the 5th ACM workshop on Networked systems for developing regions* (pp. 39-44). ACM.

Catota, F. E., Morgan, M. G., and Sicker, D. C. (2019). Cybersecurity education in a developing nation: the Ecuadorian environment. *Journal of Cybersecurity*, 5(1), 1-19.

Choejey, P., Fung, C. C., Wong, K. W., Murray, D., and Xie, H. (2015, November). Cybersecurity practices for e-Government: an assessment in Bhutan. *In The 10th International Conference on e-Business*, Bangkok, Thailand.

Cole, K., Chetty, M., LaRosa, C., Rietta, F., Schmitt, D. K., Goodman, S. E., and Atlanta, G.A (2008). Cybersecurity in Africa: An assessment. *Atlanta, Georgia, Sam Nunn School of International Affairs, Georgia Institute of Technology.* Retrieved from https://www.researchgate.net/profile/Seymour_Goodman/publication/267971678_Cybersecurity_in_Africa_An_Assessment/links/54e93dca0cf25ba91c7ef580/Cybersecurity-in-Africa-An-Assessment.pdf

Department of Communications Republic of South Africa. (2010). *Draft Cyber Security Policy*. Pretoria: Government Gazette. Retrieved from file:///C:/Users/01414525/Downloads/government-gazette-ZA-vol-536-no-32963-dated-2010-02-19.pdf

Department of Telecommunications and Postal Services. (2017). A Baseline Study on Cyber Security Readiness. Pretoria: Department of Telecommunications and Postal Services. Retrieved from https://www.cybersecurityhub.gov.za/images/docs/Cyber-Readiness-Report.pdf

Dlamini, I. Z., Taute, B., and Radebe, J. (2011). Framework for an African policy towards creating cyber security awareness. Retrieved from https://researchspace.csir.co.za/dspace/bitstream/handle/10204/5163/Dlamini_2011.pdf?sequence=1

Dodge, R., Toregas, C., and Hoffman, L. J. (2012). Cybersecurity Workforce Development Directions. *Proceedings of the Sixth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2012)* (pp. 1-12). Retrieved https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/costis_-_cybersecurity_workforce_development_directions_0.pdf

Gibson, D., Anand, V., Dehlinger, J., Dierbach, C., Emmersen, T., and Phillips, A. (2019). Accredited Undergraduate Cybersecurity Degrees: Four Approaches. *Computer*, 52(3), 3847.

ITU (2011) *National cybersecurity strategy*. Retrieved from http://www.itu.int/ITUD/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

Kessler, G. C., and Ramsay, J. D. (2014). A proposed curriculum in cybersecurity education targeting homeland security students. *In 2014 47th Hawaii International Conference on System Sciences* (pp. 4932-4937). IEEE.

Manson, D., and Pike, R. (2014). The case for depth in cybersecurity education. *ACM Inroads*, 5(1), 47-52.

Mouheb, D., Abbas, S., and Merabti, M. (2019). Cybersecurity Curriculum Design: A Survey. *In Transactions on Edutainment* XV (pp. 93-107). Springer, Berlin, Heidelberg

Muller, L. P. (2015). *Cyber security capacity building in developing countries: challenges and opportunities.* Norwegian Institute of International Affairs. Retrieved from https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/284124/NUPI+Report+03-15-Muller.pdf?sequence=3

National Academics of Science Engineering Medicine. (2018). *Globalization of Technology: International Perspectives.* Retrieved from https://www.nap.edu: https://www.nap.edu/read/1101/chapter/2

National Cyber Security Strategy 2016-2021 HM Government (2016) Accessed Dec 2016. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016to-2021

Newhouse, W., Keith, S., Scribner, B., and Witte, G. (2017). *National initiative for cybersecurity education (NICE) cybersecurity workforce framework.* NIST Special Publication, 800, 181.

Parker, A., and Brown, I. (2018). Skills Requirements for Cyber Security Professionals: A Content Analysis of Job Descriptions in South Africa. *In International Information Security Conference* (pp. 176-192). Springer, Cham.

Paulsen, C., McDuffie, E., Newhouse, W., and Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. *Security & Privacy*, 10(3), 76-79.

Quezada-Sarmiento, P. A., Enciso-Quispe, L. E., Garbajosa, J., and Washizaki, H. (2016). Curricular design based in bodies of knowledge: Engineering education for the innovation and the industry. *In 2016 SAI Computing Conference (SAI)* (pp. 843-849).

Rowe, D. C., Lunt, B. M., and Ekstrom, J. J. (2011, October). The role of cyber-security in information technology education. *In Proceedings of the 2011 conference on Information technology education* (pp. 113-122). ACM.

Ruiz, R. (2019, January). A Study of the UK Undergraduate Computer Science Curriculum: A Vision of Cybersecurity. *12th International Conference on Global Security, Safety and Sustainability* (ICGS3) (pp. 1-8).

Soomro, Z. A., Shah, M. H., and Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management,* 36(2), 215-225.

Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. *African Journal of Information and Communication*, 20, 113-132.

Van Vuuren, Joey Jansen, and Louise Leenen. (2018). Cybersecurity Capability and Capacity Building for South Africa. *IFIP International Conference on Human Choice and Computers*. Springer, Cham, 2018.

Von Solms, R., and Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security,* 38, 97-102.