# A Reference Point for Designing a Cybersecurity Curriculum for Universities

Adéle Da Veiga, Elisha Ochola, Mathias Mujinga, Keshnee Padayachee, Emilia Mwim, Elmarie Kritzinger, Marianne Loock, Peeha Machaka

# A Reference Point for Designing a Cybersecurity Curriculum for Universities

Adéle da Veiga[0000-0001-9777-8721] Elisha Ochola [0000-0001-8912-1578] Mathias Mujinga [0000-0001-6560-8082] Keshnee Padayachee [0000-0001-7056-4723] Emilia Mwim [0000-0002-1690-7518] Elmarie Kritzinger [0000-0002-5141-4348] Marianne Loock [0000-0001-8005-716X] Peeha Machaka [0000-0003-42513-7318]

Security4U Research Group, School of Computing, College of Science, Engineering and Technology, UNISA, South Africa
dveiga@unisa.ac.za, Ocholeo@unisa.ac.za, mujinm@unisa.ac.za, Padayk@unisa.ac.za, mwimen@unisa.ac.za, Kritze@unisa.ac.za, Loockm@unisa.ac.za, machap@unisa.ac.za

**Abstract.** The objective of this study is to propose a cybersecurity curriculum from a best practice perspective for universities and other higher educational institutions. Cybersecurity is a fast-growing part of the overall job market and cybersecurity skills shortage is a factor that needs attention worldwide. An updated approach is needed to build the cybersecurity labour force. A scoping literature review was applied on academic databases for proposed cybersecurity skills curricula. It was also applied on cybersecurity curricula offered by top universities as well as by studying cybersecurity curriculum frameworks and guidelines. The knowledge, skills, abilities and modules from the aforementioned were integrated to compile a holistic reference point for a cybersecurity curriculum. The study found that there is a global need for cybersecurity degrees and specifically for African countries like South African. More cybersecurity professionals need to be trained in the necessary technical abilities, combined by the necessary soft skills to be productive and fill the gaps in industry. This is possible by concentrating on this study's proposal namely a reference point for cybersecurity modules to be included in a cybersecurity curriculum.

**Keywords:** cybersecurity, curriculum, skills, education

## 1 Introduction

Cybersecurity skills challenges and a shortage of cybersecurity employees are experienced globally by organisations. It is estimated that there is a shortage of 3.12 million cybersecurity professionals across the globe [1]. The ISC found in their study that the cybersecurity skills workforce must be expanded by at least 89% to address the skills shortage, specifically in regions such as the Asia Pacific, followed by Latin America, North America and Europe [1]. In another study conducted by Check Point, 67% of the

participating IT professionals across the world indicated that their staff lacked cybersecurity skills, with a continent-wide concern in Africa [2]. The African workforce will be expanding to represent 15% of the world's working population, with approximately 60% of Africa's population being under the age of 25 by 2030 [3]. With 87% of CEOs in Africa being concerned about the availability of key skills required on the continent [4], Africa has a unique challenge in this regard. While there is a gap in cybersecurity skills worldwide, studies also show that cybersecurity knowledge is one of the fastest growing skills required within public, private and government sectors [5]. Cybersecurity skills required range from technical skills, such as network and database skills, to non-technical skills, such as cybersecurity strategy, management, project management, training risk assessments and legal requirements [5]. One way to decrease the current cybersecurity skills shortage is through education. The need for cybersecurity education within the higher education sectors is growing rapidly [6]. It is therefore vital that universities and tertiary colleges adopt new curricula to address the cybersecurity skills shortage [2]. The responsibility to build the cybersecurity profession is partly that of the education system and education institutions [4]. In a study by Kaspersky, 62% of IT professionals indicated that education establishments have a key responsibility to train cybersecurity professionals, with only a third of the responsibility placed on industry [6].

While there is no universal curriculum for cybersecurity [7], there is a need for a holistic view to consider the content of guidelines such as CSEC2017 [8], but also the content that is currently offered by universities, and in addition also the work that is proposed by academic researchers for a cybersecurity curriculum, thereby providing an integrated point of reference. A consolidated view of cybersecurity skills as proposed in academic research and what is offered in practice by universities could be used by universities as a benchmark or point of reference to define their cybersecurity qualifications in order to aid in closing the cybersecurity skills gap. This research provides universities with a guideline for a cybersecurity curriculum from a best practice perspective, but also from an operational perspective as to what academic institutions are currently offering. It is of specific importance for countries like South Africa who also requires cybersecurity skills, but where there is a lack of cybersecurity degrees offered at tertiary institutions as found in this study.

## 2 Research aims

In this research a scoping literature review [9] was applied to propose a reference point for a holistic academic cybersecurity curriculum for universities and other higher education institutions. The scoping review included:

- academic databases for proposed cybersecurity skills curricula;
- cybersecurity curricula offered by top universities; and

- cybersecurity curriculum frameworks and guidelines.

The results are consolidated to synthesise and propose a comprehensive point of reference for a cybersecurity curriculum for a tertiary educational context.

## 3 Background

Countries invest in acquiring modern technologies to secure their infrastructure within cyberspace. However, the success of these technologies depends on professionals with the appropriate cybersecurity related skills, knowledge and abilities for implementation. The cybersecurity skills shortage phenomenon, with few professionals having the skills and knowledge to protect networks, systems and data against malicious cyber attacks, arising from cyber warmongers, terrorists and cybercriminals. The cybersecurity skills gap has been recognised as a national vulnerability requiring a resolution in the UK government's cybersecurity strategy. The US government echoes the same sentiment, pointing out the need for qualified cybersecurity professionals [10]. Statistics show that the cybersecurity professionals shortage in the global labour market was at 2.93 million in 2018 [1], with a further 3.5 million global vacant positions for cybersecurity professionals estimated for 2021 [11]. $(ISC)^2$ [1] reports that 63% of their respondents confirmed a shortage of dedicated cybersecurity staff in their organisations; Capgemini [12] reports a widening digital gap for 55% of companies, with cybersecurity topping the demand list; Oltsik [13] observes that the shortage has impacted 70% of organisations over the past few years. With increased cybersecurity attacks and a shortage of cybersecurity skills, there is a great need for cybersecurity education.

Technologies and digital device adoption in South Africa (SA) has introduced diverse conveniences. However, this has also opened the doors for numerous cybercrime attacks on a global scale. High-profile data breaches have also been experienced in SA in recent years. A leakage of personal data affecting over 60 million users occurred in October 2017 [14]. The 2013 Protection of Personal Information (POPI) Act came to effect for the protection of personal information, including strengthening of security controls. However, its implementation has been slow, with only certain provisions currently implemented. In 2015, the government further responded by proposing the National Cybersecurity Policy Framework (NCPF) [15], which is yet to be implemented. The country is experiencing a lack of a skilled workforce, and cybersecurity professionals are among those in high demand. There is a need to strengthen the cyber talent pipeline, with a focus on a cybersecurity workforce. ICT technology advancements, regulations, cybersecurity incidents and increasing digitisation have shaped the cybersecurity labour market demand. The education and training of adequately skilled cybersecurity professionals is vital to fend off the global increase in sophisticated cyber attacks that have crippling effects on our way of life.

# 4 Research methodology

## 4.1 Research method

A scoping literature review [9] method was applied. The scoping review included three phases with a review of (a) cybersecurity curricula proposed in academic publications in the academic databases using the PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses) method, section 4.2; (b) cybersecurity curricula of universities in South Africa and globally applying the Time Higher Education university ranking, section 4.3; and (c) best practice and industry frameworks for cybersecurity curricula, section 4.4.

## 4.2 Academic publications defining cybersecurity curricula

All academic studies that have considered a cybersecurity curriculum were eligible for the scoping review. The following search terms: [All: "cybersecurity curriculum"] OR [All: "cyber security curriculum"] AND [Publication Date: (01/01/2015 TO 12/31/2020)] were used. The databases selected for this review included ACM, IEEE and Scopus.

**Table 1.** Inclusion and exclusion criteria

| Inclusion criteria | Exclusion criteria |
|---|---|
| **IC1**: Journal articles, conference proceedings, book chapters, reports | **EX1**: Posters, websites, keynote speeches |
| **IC2**: Empirical, theoretical or case study works on a cybersecurity curriculum design | **EX2**: Pedagogical methods (e.g. lab exercises), standalone modules (i.e. a discussion on the development of a standalone module), applications in other fields (e.g. engineering, healthcare), awareness campaigns, community involvement and training for professionals |
| **IC3**: Practices that have been implemented at tertiary level | **EX3:** Practices at school level |
| **IC4**: Articles written in 2015-2020 | **EX4**: Articles prior to 2015 |

Using the PRISMA method, the process involved screening the papers by reviewing the title and the abstract's fitness for the study based on the criteria outlined in Table 1. The articles that remained were verified for suitability by reviewing the full-text version. The next step involved reviewing each article for their quality and relevance using five questions, Table 2, as adopted from Salleh et al. (2011). This checklist was appropriate, as the original study also considered pedagogical issues in higher education in computer science.

**Table 2.** Study quality checklist (adapted from Salleh et al. [16] and Kmet et al. [17])

| Quality criteria | Reference |
|---|---|
| **QC1**: Was the article peer-reviewed? | [16] |
| **QC2**: Were the aims clearly stated? | [16] |

| | |
|---|---|
| **QC3**: Is the context clear? For example, the setting should be within a university. | [17] |
| **QC4**: Is there a connection to a theoretical framework/wider body of knowledge? | [17] |
| **QC5**: Do the findings resonate with other research findings? | [16] |

### 4.3 Results

The search and appraisal strategy applied generated a sample of **n = 8** studies from the respective databases, Table 3. The process involved three researchers who searched each database independently. If there was a dispute regarding a paper, the researchers collaborated and refined the exclusion criteria to focus on papers that provided a description or proposal of a curriculum in cybersecurity. Each researcher then considered the quality criteria and excluded further papers (excluded on QC3 and QC4). After consolidating the list of articles, it was found there was one duplicate, and this was eliminated, which generated a final sample of **n = 7**.

**Table 3.** PRISMA method

| Database | #Records identified through database searching | #Records after duplicates removed | #Records screened | #Records excluded (exclusion/inclusion criteria) | #Full-text articles assessed for eligibility | #Full-text articles excluded, with reasons | #Articles included in the synthesis |
|---|---|---|---|---|---|---|---|
| IEEE | 13 | 13 | 13 | 9 | 4 | $2^{QC3}$ | 2 |
| ACM | 40 | 40 | 40 | 17 | 23 | $20^{QC3\&4}$ | 3 |
| SCOPUS | 66 | 66 | 66 | 59 | 9 | $6^{QC3\&4}$ | 3 |

Švábenský et al. [18] conducted a systematic review; however, while their search was wider, they only considered relevant conference papers (2010-2019). Their work provides a good basis toward this end and leveraged the CSEC2017 framework to identify the most common topics that were covered in cybersecurity curricula as summarised in Table 4. Bell and Oudshoorn [19] suggest that the methodology of developing a new programme should involve determining the focus areas and a consideration of exemplar programmes which could assist in that process. The Northwest Missouri State University offers a Bachelor of Science degree in cybersecurity [19] with a consideration of the eight knowledge areas of CSEC2017. The criteria proposed by the Accreditation Board for Engineering and Technology (ABET) [20] was also employed as well as input from industry stakeholders. Asghar and Luxton-Reilly [21] provide an overview of a Cybersecurity Master's Programme (University of Auckland) based on the ITiCSE framework as a case study. The six courses comprise four compulsory subjects (based on system security and security management) and ten electives (students choose two courses that focus on specialist strengths alongside the core knowledge). While the previous studies considered frameworks from a teaching and learning perspective, Jones et al. [22] embarked on a survey to identify the most relevant knowledge, skills, abilities (KSAs) that should be prioritised for a cybersecurity curriculum in order to prepare graduates for careers in cybersecurity using the NICE framework's KSAs as a basis. Buckley and Zalewski [23] highlight issues of teaching basic principles of cybersecurity at Florida Gulf Coast University. The curriculum is based on the CSEC2017

guidelines. They also compare CSEC2017 and $(ISC)^2$/CPHC [24] as guidelines for curriculum development and conclude that the former is more curriculum based while the latter is more technology based. The authors developed two courses as part of an undergraduate Software Engineering programme: "Security Software" and "Introduction to Cybersecurity". Asghar, Swain and Biswal [25] report on the design and development of a cybersecurity concentration course for undergraduate students. The programme is based on the ABET accreditation at the South Carolina State University. In this case 15% of the coursework was devoted to cybersecurity. This programme was based on existing curricula and discussions with industry and scholars. While some curriculum models are based on established frameworks, other case studies provide approaches based on alternative perspectives. Santos, Pereira and Mendes [26] propose a flexible curriculum based on the framing of prevention, detection and response for a graduate-level curriculum in cybersecurity. The core curriculum should consider prevention, detection and response.

**Table 4.** Academic cybersecurity curricula and related modules

| Database | Description | Frameworks | Overview of modules |
|---|---|---|---|
| ACM | Predominately tertiary education in the USA [18] | CSEC 2017 Framework. A review of SIGCSE and ITiCSE conferences was also considered. | The primary cybersecurity topics: Secure Programming and Software Development, Network Security and Monitoring, Human Aspects in Security, Cyber-Attacks, Malware, Hacking, Offensive Security and Exploitation, Cryptography, Authentication and Authorization. |
| IEEE | Bachelor of Science degree in cybersecurity (Northwest Missouri State University) [19] | CSEC2017 Programme outcomes adopted from the ABET cybersecurity accreditation criteria | BSc programme structure: Introduction to Cybersecurity, Secure Programming, Incident Response, Cyber Risk Management, Digital Forensics and Ethical Hacking. Existing modules include: Professional Ethics, General Psychology, General Statistics, Discrete Mathematics, Computer Programming I and II, Data Structures, IT Hardware and Software, Network Fundamentals, Computer Organization, Database Systems, Operating Systems, Secure Systems Administration and Applied Cryptography. |
| ACM | Cybersecurity master's programme (University of Auckland) [21] | ITiCSE 2018 | Compulsory modules: Information Security, System Security, Network Security and Cryptographic Systems and ten electives: Smartphone Security, Human Computer Interaction, Advanced Analysis of Algorithms, Software Tools and Techniques, Data Communications, Information Systems Research, Telecommunications Management, Enterprise Systems, Research Methodology – Quantitative and Research Methodology – Qualitative. Students to select two of the ten electives. |
| ACM | Proposed KSAs of cybersecurity curriculum [22] | NICE Framework | The KSAs that should be prioritised when developing cybersecurity course curricula relate to networks, vulnerabilities, programming and communication skills. |
| Scopus | Part of an undergraduate software engineering programme (Florida Gulf Coast University) [23] | CSEC2017 (IEEE Computer Society, 2014) (Data Communication Networks: Open System Interconnection (OSI); Security Structure and Applications, 1991) | Software Security course with Cryptography, Network Security Protocols and Detection (Penetration Testing and Threat Modelling). Introduction to Cyber Security course with fundamental cybersecurity principles, practices and security controls and includes a cybersecurity laboratory (i.e. hands-on activities). The notion of protection mechanisms for implementing security services are covered from a software development cycle perspective. |

| | | | |
|---|---|---|---|
| Scopus | Cybersecurity curriculum for computer science major students (South Carolina State University) [25] | ABET accredited computer science programme | The embedded programme courses include Introduction to Cybersecurity, Computer Forensics, Cryptography and Network Security, Application and Data Security with Privacy, Management of Information Security and a Cyber Security Capstone project. |
| IEEE | Proposed graduate-level curriculum certificate [26] | Based on the Framing of Information Security Management: Prevention, Detection and Response | A graduate-level curriculum comprising the following areas: Prevention (e.g. penetration testing, ethical hacking); detection (e.g. intrusion detection systems) and response (e.g. digital forensics and incident response). Other areas proposed include cultural and global standardisation, legal issues, awareness, counter forensics and the theory of computer forensics. |

The programmes listed in Table 4 highlight the wide scope of cybersecurity qualifications and various options of module selection of topics available to curriculum developers. Seven core modules crosscut these curricula, namely networks, cryptography, cybersecurity, forensics, programming human aspects and ethical hacking, with 34 unique modules across the seven curricula. It is worth pointing out that each of these curricula listed in Table 4 is based on a framework.

### 4.4 Cybersecurity curricula of universities

The Time Higher Education (THE) University rankings rank universities based on their academic research performance and their overall reputation and ratings by members of the academic community around the world [27]. Undergraduate programmes that are based solely on cybersecurity or incorporate an aspect of it were included in the scope. There were no undergraduate programmes in South African universities that focused solely on cybersecurity, but undergraduate programmes in the listed universities had modules that covered aspects of cybersecurity. Since a complete undergraduate course in cybersecurity was not found, it was concluded that South African universities do not have a formal undergraduate course in cybersecurity. Three websites were used to identify international universities for inclusion in the scope: www.educations.com; www.bachelorstudies.com; and www.barchelorportal.com. The researchers searched for 3- and 4-year bachelor's degrees in cybersecurity that are taught in English. educations.com returned 113 results, bachelorstudies.com returned 19 results and bachelorportals.com returned 64 results. The results were sorted by relevance and the THE university ranking. The cybersecurity programmes of the top 5 highly ranked universities according to THE [27] were then reviewed, with the results summarised in Table 5.

**Table 5.** Cybersecurity university degrees and related modules

| University | Degree | University ranking | Overview of modules |
|---|---|---|---|
| Cardiff University | Computer Science with Security and Forensics [28] | 191 | Security, Forensics, Cryptography, Probability, Discrete Mathematics, Programming |
| Macquarie University | Bachelor of Commerce with a Major | 195 | Cyber Security, Cybercrime, Information Systems and Business Processes, Blockchain for Business, |

| University | Degree | University ranking | Overview of modules |
|---|---|---|---|
| | in Cyber Security Governance [29] | | Cyber Security and Privacy, Cyber Security Governance and Ethics, Information Systems Audit and Assurance |
| University of Winchester | BSc (Hons) Cyber Security [30] | 201-300 | Cyber Security and Networks, Artificial Intelligence, Network Security, Secure Systems Architectures, Risk Management and Cyber Security, Penetration Testing, Digital Forensic Investigation, Cyber Law and the Regulation of the Information Society, Globalised Crime, Organised Crime and Cyber Crime |
| Deakin University | Bachelor of Criminology/Bachelor of Cyber Security [31] | 251-300 | Crime and Criminology, Criminal Justice, Programming, Cyber Security, Discrete Mathematics, Secure Networking, Secure Coding, Computer Crime and Digital Forensics, Malware and Network Forensics, Ethical Hacking |
| Flinders University | Bachelor of Information Technology (Network & Cybersecurity Systems) [32] | 251-300 | Computing, Computer Programming, Electronics, Networks and Cybersecurity, Mathematics, Data Science, Software Engineering, Computer Networks, Cybersecurity, Enterprise Information Security |

Cybersecurity or Security was the module that was most represented, with four of the university curricula including it. This was followed by the modules Forensics, Programming, Networks, Mathematics (including Discrete Mathematics) and Cyber Crime, which were each included in the curricula of three of the universities. There were 18 unique modules across the five universities.

### 4.5 Best practice and industry frameworks for cybersecurity curricula

Organisations can use different international best practices to guide them in improving cybersecurity, education resources and curricula [33, 34]. According to Caruso [35], best practices have a wide scope. For this paper cybersecurity best practices are defined as documents that have structures, processes, practices and technologies that can aid in improving cybersecurity within an organisation. Security best practices can be seen as guidelines on security topics that are relevant and important within the industry sectors. It is therefore critical that educational curricula at higher education institutions be based on industry-required knowledge and skills. Best practices can be used as a basis to identify cybersecurity knowledge and transfer skills.

Two approaches can be used when designing a cybersecurity curriculum: 1) Using one existing best practice for the curriculum or 2) using a combination of frameworks and best practices to create a customised cybersecurity curriculum. There are numerous ways and methods to group and categorise cybersecurity topics relevant to educational curriculum development. In this research nationally accepted cybersecurity best practices were consulted to identify relevant cybersecurity topics and different options to group these topics. International documents consulted include Cybersecurity Curricular Guidelines (2017) [36]; CyBOK (2019); ISSP - Information Security Skills Framework (2010) [37]; NIST Cyber Security Framework (2014) [38] and Soc2 [39]. These documents were analysed to identify the different security related topics. The process of data

saturation was used when identifying these topics. Data saturation is reached when results are repeating with low new contribution to the findings. Saturation was reached after the five mentioned best practices [40]. Table 6 depicts the list of security topics derived from the collection documents. Some topics are not directly related to security such as communication or research, but is contextualised to security. For example, how to conduct research in cybersecurity or implementation of secure communications in networks or conducting awareness communication of the cybersecurity policy. Additional security topics can be added to this list. Within the design phase of a cybersecurity related curriculum, the topics (in Table 6) can be a baseline for the knowledge and skills based planning.

**Table 6.** Security related topics

| | | |
|---|---|---|
| Access control | Improvements | Recovery planning |
| Adversarial behaviour | Incident management | Regulatory aspects |
| Anomalies & events | Information assurance methodologies | Research |
| Asset analysis & management | Information security strategy | Response planning |
| Attacks & defences | Infrastructure security | Risk assessment |
| Audit, assurance & review | Intrusion detection | Risk management |
| Awareness & training | Investigation | Secure development |
| Business continuity management | Law & regulation | Secure operations management |
| Business environment | Maintenance | Security architecture |
| Business improvements | Malware | Security incident handling |
| Communications | Management | Security innovation |
| Component & connection security | Management strategy | Security monitoring |
| Connection security | Mitigation | Security software life cycle |
| Cryptography | Network security | Security testing |
| Data security | Operational security management | Service delivery |
| Detection processes | Organisation security | Social security |
| Disaster recovery | Performance monitoring | Software security |
| Distributed systems security | Physical security | System security |
| Encryption | Policy & standards | Telecommunications |
| Firewalls | Privacy & online rights | Third party management |
| Forensics | Processing monitoring | Two factor authentication |
| Governance | Protection & procedures | Virtualisation |
| Hardware security | Protective technology | Vulnerability assessment |
| Human security | Quality assurance | Web & mobile security |

## 5 Reference point for a cybersecurity curriculum

The modules derived from the 7 literature review papers as well as the modules derived from the 5 universities were consolidated to compute a unique list of 49 modules. The occurrence of each module across the 7 literature review papers (column A) and 5 university curricula (column B) were counted to determine the number of instances each module occurred across the curricula. The modules that occurred the most frequently were considered as the core or critical modules for inclusion in the cybersecurity curriculum. The framework topics from Table 6 were mapped to the list of 49 modules and a match was indicated by a “X” in column C. Only business continuity management, disaster recovery, security innovation, service delivery and third party management did

not map to any of the modules and were thus added as possible additional modules, thereby increasing the module list to 53. The last column, "Total", portrays the modules that were represented in the literature review curricula and the university curricula and map to a topic in a framework. The modules are ranked according to the last total column in terms of the number or occurrence across the academic databases, best practice and existing curricula offered by universities covered in the scope of the study. This gives an indication of the most common modules that are currently included in proposed curricula, presenting an integrated view. Table 7 therefore outlines 53 modules in order of three tiers:

- Tier 1: Core modules for a cybersecurity curriculum
- Tier 2: Fundamental modules for a cybersecurity curriculum
- Tier 3: Elective modules for a cybersecurity curriculum

**Table 7.** Reference point for a cybersecurity curriculum

| | **Modules** | **A** | **B** | **Total** | **Framework mapping to unique modules** | **C** | **Total** |
|---|---|---|---|---|---|---|---|
| TIER 1 | 1. Networks | 6 | 3 | 9 | Network Security; Firewalls; Intrusion Detection; Component and Connection Security; Anomalies and Events; Adversarial Behaviour | X | 10 |
| | 2. Cryptography | 5 | 1 | 6 | Cryptography; Encryption | X | 7 |
| | 3. Cyber Security | 3 | 4 | 7 | | | 7 |
| | 4. Forensics | 3 | 3 | 6 | Forensics; Investigation | X | 7 |
| | 5. Programming | 3 | 3 | 6 | | | 6 |
| | 6. Crime | 1 | 3 | 4 | | | 4 |
| | 7. Mathematics | 1 | 3 | 4 | | | 4 |
| | 8. Architecture | 1 | 1 | 2 | Security Architecture | X | 3 |
| | 9. Ethical Hacking | 2 | 1 | 3 | | | 3 |
| | 10. Human Aspects | 2 | | 2 | Human Security; Social Security | X | 3 |
| | 11. Law/legal | 1 | 1 | 2 | Law & Regulation; Regulatory Aspects | X | 3 |
| | 12. Privacy | 1 | 1 | 2 | Privacy & Online Rights | X | 3 |
| | 13. Risk Management | 1 | 1 | 2 | Risk Management; Risk Assessment; Mitigation | X | 3 |
| | 14. Software Tools and Techniques, Engineering | 1 | 1 | 2 | Software Security | X | 3 |
| TIER 2 | 15. Audit and Assurance | | 1 | 1 | Audit, Assurance & Review, Information Assurance Methodologies; Quality Assurance | X | 2 |
| | 16. Authentication and Authorisation | 1 | | 1 | Access Control; Two-Factor Authentication | X | 2 |
| | 17. Awareness | 1 | | 1 | Awareness & Training | X | 2 |
| | 18. Business Processes | | 1 | 1 | Business Environment | X | 2 |
| | 19. Communication Skills | 1 | | 1 | Communications | X | 2 |
| | 20. Computing | 1 | 1 | 2 | | | 2 |
| | 21. Cyber Attacks | 1 | | 1 | Attacks & Defences | X | 2 |
| | 22. Data Science | 1 | 1 | 2 | | | 2 |
| | 23. Data Structures | 1 | | 1 | Data Security | X | 2 |
| | 24. Enterprise Security | | 1 | 1 | Organisation Security; Business Improvements; Asset Analysis and Management; Improvements; Infrastructure Security; Maintenance; Operational Security Management; Secure Operations Management | X | 2 |

| | Modules | A | B | Total | Framework mapping to unique modules | C | Total |
|---|---|---|---|---|---|---|---|
| | 25. Ethics | 1 | 1 | 2 | | | 2 |
| | 26. Incident Response | 1 | | 1 | Incident Management; Security Incident Handling; Detection Processes | X | 2 |
| | 27. IT Hardware and Software | 1 | | 1 | Hardware Security; Physical Security; Protective Technology | X | 2 |
| | 28. Malware | 1 | | 1 | Malware | X | 2 |
| | 29. Management of Information Security | 1 | | 1 | Management; Management Strategy; Governance; Information Security Strategy; Policy & Standards; Protection and Procedures | X | 2 |
| | 30. Prevention, Detection | 1 | | 1 | Response Planning; Recovery Planning | X | 2 |
| | 31. Research Methodology | 1 | | 1 | Research | X | 2 |
| | 32. Smartphone Security | 1 | | 1 | Web & Mobile Security | X | 2 |
| | 33. Software Engineering/Development | 1 | | 1 | Secure Development; Security Software Life Cycle | X | 2 |
| | 34. System Security | 1 | | 1 | System Security; Distributed Systems Security; Security Testing; Performance Monitoring; Processing Monitoring; Security Monitoring | X | 2 |
| | 35. Telecommunications Management | 1 | | 1 | Telecommunications | X | 2 |
| | 36. Vulnerabilities | 1 | | 1 | Vulnerability Assessment | X | 2 |
| TIER 3 | 37. Advanced Analysis of Algorithms | 1 | | 1 | | | 1 |
| | 38. Artificial Intelligence | | 1 | 1 | | | 1 |
| | 39. Block Chain | | 1 | 1 | | | 1 |
| | 40. Cultural and Global Standardisation | 1 | | 1 | | | 1 |
| | 41. Database Systems | 1 | | 1 | | | 1 |
| | 42. Electronics | | 1 | 1 | | | 1 |
| | 43. General Psychology | 1 | | 1 | | | 1 |
| | 44. General Statistics | 1 | | 1 | | | 1 |
| | 45. Information Security | 1 | | 1 | | | 1 |
| | 46. Operating Systems | 1 | | 1 | Virtualisation | | 1 |
| | 47. Penetration testing | | 1 | 1 | | | 1 |
| | 48. Probability | | 1 | 1 | | | 1 |
| | 49. Secure Systems Administration | 1 | | 1 | | | 1 |
| | 50. | | | | Business Continuity Management and Disaster Recovery | X | 1 |
| | 51. | | | | Security Innovation | X | 1 |
| | 52. | | | | Service Delivery | X | 1 |
| | 53. | | | | Third Party Management | X | 1 |

The research found that there is consensus that cybersecurity courses at undergraduate level will require a computing background and that cybersecurity courses have been embedded into existing Computer Science programmes. The modules in table 7 range from specific cybersecurity topics like networks, ethical hacking and cyber attacks to more general topics like awareness, communication skills, electronics and general psychology. Therefore the development of any new cybersecurity curriculum will most likely have to include the core modules and a specific specialisation area as well as target a particular cohort of students using the fundamental and elective modules. A

cybersecurity curriculum could be based on existing frameworks as mapped in Table 7, but it is proposed that these need to include industry stakeholders to review the relevance of topics proposed. From a pragmatic viewpoint as illustrated in the case study of Buckley and Zalewski [23], the importance of leveraging existing strengths in the institution should be incorporated when designing the cybersecurity curriculum. This study identified that there is a lack of cybersecurity degrees in South African universities and the proposed modules in table 7 for such a curriculum could serve as a reference point.

Alsmadi and Zarour [41] highlighted some issues with cybersecurity programs. First, the divide between theoretical knowledge and the practical skills. It is recommended that course material must consider knowledge, skills and ability (i.e. be able to innovate). Second the gap between industrial requirements and the knowledge base of students. The third problem is the lack of planning with respect to how to evolve with industry's needs. This study proposed a reference point that could be used towards the development of a cybersecurity curriculum that intends to be a strategy that addresses the first two challenges. In this demonstration, the reference point identified core modules such as Networks, Cryptography, Cybersecurity, Forensics and Programming, as obtained from current cybersecurity curricula and best practices. The development of the reference point involved a three-pronged approach using the PRISMA method for academic publications, best practice and industry frameworks as well as existing cybersecurity curricula of universities. It is envisaged that the proposed strategy can be used by academic institutions as a point of departure towards defining cybersecurity curricula, to map them for completeness and provide organisations with a point of reference for the cybersecurity skills they need. The literature review is useful in assisting further research and the aggregation and statistical support may be used by some when justifying and proposing new or enhanced cybersecurity curriculum. A limitation of this study is that only a literature review was conducted and with a lack of a cooperative approach with industry that could address the last challenge identified by Alsmadi and Zarour [41]. Future studies will extend the reference point to include qualitative and quantitative input that will assist in mapping the evolving needs of industry with theoretical knowledge and practice.

## 6 Conclusion

This study proposed a reference point for a cybersecurity curriculum that may be utilised within higher education institutions to graduate more cybersecurity professionals. A reference point is proposed for cybersecurity modules to be included in a cybersecurity curriculum that contributes to the cybersafety body of knowledge. The proposed curriculum focuses on core modules such as Networks, Cryptography, Cybersecurity, Forensics and Programming, as obtained from current cybersecurity curricula and best practices. The research included a three-phased approach using the PRISMA method for academic publications, best practice and industry frameworks as well as existing cybersecurity curricula of universities. It is envisaged that the proposed cybersecurity curriculum can be used by academic institutions to define their cybersecurity curricula,

to map them for completeness and provide organisations with a point of reference for the cybersecurity skills they need.

## References


1. (ISC)2: Cybersecurity Professionals Stand Up to a Pandemic. https://www.trendmicro.com/closethegap/wp-content/uploads/2018/11/2018-ISC2-Cybersecurity-Workforce-Study.pdf, last accessed 2021/03/09.
2. Kagwiria, C.: Cybersecurity skills gap in Africa, https://www.afralti.org/cybersecurity-skills-gap-in-africa/, last accessed 2021/03/09
3. Shango, D.: Why the skills gap remains wider in Africa, https://www.weforum.org/agenda/2019/09/why-the-skills-gap-remains-wider-in-africa/, last accessed 2021/03/09.
4. PricewaterhouseCoopers: CEOs' curbed confidence spells caution, https://www.pwc.com/gx/en/ceo-survey/2019/report/pwc-22nd-annual-global-ceo-survey.pdf, last accessed 2021/03/09.
5. Furnell, S., Bishop, M.: Addressing cyber security skills: the spectrum, not the silo. Comput. Fraud Secur. 2020, 6–11 (2020).
6. Kaspersky Lab: The Cybersecurity Skills Gap: a Ticking Time Bomb, https://media.kaspersky.com/uk/Kaspersky-Cyberskills-Report_UK.pdf, last accessed 2021/03/09.
7. Bishop, M., Burley, D., Futcher, L.A.: Cybersecurity Curricular Guidelines. In: Ismini, V. and Furnell, S. (eds.) Cybersecurity Education for Awareness and Compliance. pp. 158–180. IGI Global, Hershey PA, USA (2019)
8. Joint Task Force on Cybersecurity Education: Curricula 2017 Cybersecurity Curriculum, http://www.csec2017.org/, last accessed 2021/03/09.
9. Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G., Grp, P.: Preferred Reporting Items for Systematic Reviews and Meta-Analyses Ann. Intern. Med. 89, 264–270 (2009).
10. De Zan, T.: Mind the Gap: The Cyber Security Skills Shortage and Public Policy Interventions, https://ora.ox.ac.uk/objects/uuid:e9699fc6-279c-4595-b707-7fd0acc487b3/download_file?file_format=pdf&safe_filename=cyber-ebook-definitivo.pdf&type_of_work=Working+paper, last accessed 2021/03/09.
11. Morgan, S.: 2018-2021 Cybersecurity Jobs Report, https://herjavecgroup.com/wp-content/uploads/2018/11/HG-and-CV-Cybersecurity-Jobs-Report-2018.pdf, last accessed 2021/03/09.
12. Buvat, J., Turner, M., Slatter, M., Ramya Krishna Putter: Cybersecurity Talent: The big gap in cyber protection, https://www.capgemini.com/wp-content/uploads/2018/02/the-cybersecurity-talent-gap-v8_web.pdf, last accessed 2021/03/09.
13. Oltsik, J.: The Life and Times of Cybersecurity Professionals, https://www.esg-global.com/hubfs/issa/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Nov-2017.pdf?hsCtaTracking=a63e431c-d2ce-459d-8787-cc122a193baf%7Ce74f0327-0bbc-444a-b7a8-e2cd08d1999e CtaTracking=a63e431c-d, last accessed 2021/03/09.

14. Veerasamy, N., Mashiane, T., Pillay, K.: Contextualising Cybersecurity Readiness in South Africa Namosha. In: Waag-Cowling, N. van der and Leenen, L. (eds.) Proceedings of the 14th International Conference on Cyber Warfare and Securit. ACPI (2000)
15. Sutherland, E.: Governance of Cybersecurity – The Case of South Africa. African J. Inf. Commun. 83–112 (2017).
16. Salleh, N., Mendes, E., Grundy, J.: Empirical Studies of Pair Programming for CS/SE Teaching in Higher Education: A Systematic Literature Review. IEEE Trans. Softw. Eng. 37, 509–525 (2011).
17. Kmet, L.M., Cook, L.S., Lee, R.C.: Standard quality assessment criteria for evaluating primary research papers from a variety of fields. , Edmonton: Alberta Heritage Foundation for Medical Research (AHFMR). HTA Initiative #13. (2004).
18. Švábenský, V., Vykopal, J., Čeleda, P.: What are cybersecurity education papers about? a systematic literature review of sigcse and iticse conferences. In: Proceedings of the 51st ACM Technical Symposium on Computer Science Education. pp. 2–8, Portland (2020).
19. Bell, S., Oudshoorn, M.: Meeting the Demand: Building a Cybersecurity Degree Program with Limited Resources. In: Proceedings - Frontiers in Education Conference, FIE. pp. 1–7. IEEE (2019).
20. Criteria for Accrediting Computing Programs, 2018-2019 | ABET.
21. Asghar, M.R., Luxton-Reilly, A.: A Case Study of a Cybersecurity Programme. In: Proceedings of the 51st ACM Technical Symposium on Computer Science Education. pp. 16–22. ACM, New York (2020).
22. Jones, K.S., Namin, A.S., Armstrong, M.E.: The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. ACM Trans. Comput. Educ. 18, (2018).
23. Buckley, I.A., Zalewski, J.: Course development in the cybersecurity curriculum. In: Proceedings of the LACCEI international Multi-conference for Engineering, Education and Technology. pp. 24–26 (2019).
24. CPHC: Cybersecurity Principles and Learning Outcomes for Computer Science an IT-related Degrees: A Resource for Course Designers and Accreditors. (ISC)2 and The Council of Professors and Heads of Computing (2015).
25. Swain, N., Biswal, B.: Design and development of cybersecurity concentration courses and laboratory experiences for undergraduate students. ASEE Annu. Conf. Expo. Conf. Proc. (2019).
26. Santos, H., Pereira, T., Mendes, I.: Challenges and reflections in designing Cyber security curriculum. In: 2017 IEEE World Engineering Education Conference (EDUNINE). pp. 47–51 (2017)
27. THE - Times Higher Education: World University Rankings (2020), https://www.timeshighereducation.com/world-university-rankings/2020/world-ranking#!/page/0/length/25/sort_by/rank/sort_order/asc/cols/stats, last accessed 2021/03/09.
28. Cardiff University: Computer Science with Security and Forensics (BSc) - Study - Cardiff University, https://www.cardiff.ac.uk/study/undergraduate/courses/2021/computer-science-with-

security-and-forensics-bsc, last accessed 2021/03/09.
29. Macquarie University: Bachelor of Commerce with a Major in Cyber Security Governance | Macquarie University, https://courses.mq.edu.au/2020/domestic/undergraduate/bachelor-of-commerce-cyber-security-governance, last accessed 2021/03/09.
30. University of Winchester: BSc (Hons) Cyber Security - University of Winchester, https://www.winchester.ac.uk/study/undergraduate/courses/bsc-hons-cyber-security/, last accessed 2021/03/09.
31. Deakin University: Bachelor of Criminology/Bachelor of Cyber Security | Deakin, https://www.deakin.edu.au/course/bachelor-criminology-bachelor-cyber-security, last accessed 2021/03/09.
32. Flinders University: Study the Bachelor of Information Technology (Network and Cybersecurity Systems) - Flinders University, https://www.flinders.edu.au/study/courses/bachelor-information-technology-network-cybersecurity-systems?source=ecs-int-home, last accessed 2021/03/09.
33. Ma, Q., Pearson, J.: ISO 17799: "Best Practices" in Information Security Management? In: Communications of the Association for Information Systems. pp. 577–591. Association for Information Systems (2005).
34. Coventry, L., Briggs, P., Blythe, J., Tran, M.: Using behavioural insights to improve the public's use of cyber security best practices, Northumbria (2015).
35. Osburn, J., Caruso, G., Wolfensberger, W.: The concept of "best practice": A brief overview of its meanings, scope, uses, and shortcomings. Int. J. Disabil. Dev. Educ. 58, 213–222 (2011).
36. Joint Task Force on Cybersecurity Education: CyberSecurity Curricula. ACM,IEEE-CS,AIS SIGSEC, IFIP, New York (2017).
37. Professionals, Institute of Information Security: The IISP Skills Framework-Scoring levels for Skills Framework, https://apmg-international.com/sites/default/files/documents/products/iisp_skills_framework_v1_0.pdf, last accessed 2021/03/09.
38. NIST: Framework for Improving Critical Infrastructure Cybersecurity, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf last accessed 2021/03/09.
39. AICPA: 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocu, last accessed 2021/03/09.
40. Saunders, M., Lewis, P., Thornhill, A.: Research methods for business students. Pearson Education Limited, England (2016).
41. Alsmadi, I., Zarour, M.: Cybersecurity programs in Saudi Arabia: issues and recommendations. In: 1st International Conference on Computer Applications & Information Security (ICCAIS). pp. 1–5. IEEE (2018)