Proceedings of the Eleventh International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2017)

Towards the Design of a Cybersecurity Module for Postgraduate Engineering Studies

S. von Solms[1] and L. Futcher[2]

[1]Department of Electrical Engineering Science, University of Johannesburg, Johannesburg, South Africa
[2]School of Information and Communication Technology, Nelson Mandela University, Port Elizabeth, South Africa
e-mail: svonsolms@uj.ac.za; Lynn.Futcher@mandela.ac.za

Abstract

The rate of technological development has changed and shaped the way in which individuals and businesses work and interact. The fourth industrial revolution has led to smart factories where cyber-physical systems communicate and work with each other and with humans. These advancements have largely brought forth positive change, but the dependence on the Internet also made us susceptible to cybercrimes, such as identity theft, fraud and espionage. Cybercrime is considered as possibly the greatest threat to companies worldwide, and therefore cybersecurity engineers are amongst the most sought after professionals. In South Africa, engineers are not traditionally trained in cybersecurity, but with the threat of cyberattacks in industry rising, a solid foundation in cybersecurity can equip engineering graduates to secure and protect their workplace. This paper describes the process followed toward the design of a cybersecurity module for postgraduate engineering studies to help address the shortfall of cybersecurity engineers in South Africa.

Keywords

Awareness, Cybersecurity, Curriculum design, Engineering, Postgraduate Education.

1. Introduction

The 21st century has seen the impact of technology on the modern world, including the development of the iPhone (Dilger, 2017); the rise of Facebook (Zephoria, 2017); and the Internet of Things (IoT) (Nordrum, 2016). The 4th industrial revolution, branded Industry 4.0 (BMBF, 2011), aims to integrate Information Technology (IT) and Operational Technology (OT), creating smart factories where cyber-physical systems communicate and work with each other and with humans in real time (Hermann et al., 2016). While this integration of technology is largely positive, our dependence on it has also made us vulnerable to cybercrimes, where 2015 saw over 1.5 million cyberattacks (Morgan, 2015; Nordrum, 2016). The consequences of breached home automation systems, factory floors or electronic health records can be catastrophic for individuals as well as for manufacturers. Therefore, businesses embracing the fourth industrial revolution must reconsider the re-engineering of their systems, networks and software to incorporate security across the entire lifecycle for inherent security (Morgan, 2015; Tamura, 2017).

In South Africa (SA) and globally, undergraduate Science, Technology, Engineering and Mathematics (STEM) courses, especially engineering, seldom includes specialisation topics such as cybersecurity (McGettrick, 2013). Traditional engineers are not trained in cybersecurity, evident in the worldwide demand for cybersecurity professionals. The development of a postgraduate cybersecurity module in engineering aims to provide engineers with a solid foundation on cybersecurity and to equip them to act with cybersecurity knowledge in the workplace. This paper describes the process followed toward the design of such a module. This work will contribute to cybersecurity curriculum design in engineering which could provide a roadmap for the integration of cybersecurity into formal engineering education.

2. Cybersecurity education and the need for professionals

The Joint Task Force on Cybersecurity Education (CSEC2017) defines cybersecurity as "*a computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries... It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management*" (Burley et al., 2017). In a 2015 survey, professionals named cybersecurity as the number one risk that enterprises are likely to face in the upcoming years (University of Phoenix, 2015). IoT is predicted to have more than 30 million connected devices by 2020 (Nordrum, 2016), including automated devices in the home, factory floors and streets, which can be targeted (University of San Diego, 2016). Poorly build integrated systems can have a major impact on the manufacturers as well as the individuals and businesses who use them (University of San Diego, 2016) as vulnerability increases with connection (Gardner, 2016). This integration means that cybersecurity cannot be limited to the IT industry, but that it must be included in software development, networking, risk management and human factors.

The last decade has seen a large push from industry to train cybersecurity professionals. One of the fastest growing fields globally, it is estimated to grow by 1.5 million workers worldwide by 2020 and that there will be a shortfall of nearly 700,000 security professionals (Cisco Advisory Services, 2015; Frost and Sullivan, 2015). In addition to the global shortfall, South African industries also face a challenge of retention, as cybersecurity professionals often find more lucrative offers elsewhere (Fripp, 2017). Worldwide, there exist a small number of cybersecurity undergraduate and postgraduate engineering degrees, with no known courses offered by South African universities. According to the undergraduate syllabuses of engineering courses offered by major universities in SA, no program offers a comprehensive module in cybersecurity. When considering the mismatch between cybersecurity education and industry requirements, it is imperative to integrate cybersecurity education into engineering, driven by the needs and the perspective of the engineering discipline.

3. Methodology and Research Process

The objective of this paper is to identify the knowledge areas and competencies which can be included in engineering programs in order to provide engineers with

relevant cybersecurity knowledge. With the need to integrate cybersecurity education in engineering in SA, this paper discusses the development of a postgraduate cybersecurity module for engineering students studying toward their Masters (M.Eng) in Electrical Engineering. The proposed module forms part of a course work Master's qualification where the students, typically working engineering professionals, complete a set of modules as well as a mini research dissertation over a two-year period. The methodology followed in the creation of the proposed postgraduate cybersecurity module consisted of the following steps:

- To investigate the Qualification Standard for Bachelors of Engineering (BEng) by the Engineering Council of South Africa (ECSA) to determine the educational requirements for the undergraduate Engineering degree. Determine the recommendations of ECSA for postgraduate specialisation.
- To identify knowledge areas and competencies in current cybersecurity models and to determine which will be of value to engineers and would complement the Engineering competencies according to ECSA.
- To investigate how cybersecurity knowledge and competencies can be integrated into the existing Engineering degree.
- To construct a module outline by matching knowledge areas to competencies of cybersecurity requirements for engineering.

The results of the various steps are discussed in the subsequent section.

4. Towards the cybersecurity module development

4.1. Current landscape of South African Engineering degree structure

In the Qualification Standard for Bachelor of Engineering (B.Eng), ECSA stipulates that accredited engineering programs "should not address narrow niche markets" and that broad undergraduate programs must be supported by "specialized course-based postgraduate programs" (ECSA, 2014). The program stipulates that the undergraduate program's coherent core must be in mathematics, natural sciences and engineering fundamentals to provide a solid platform for further studies and lifelong learning, where specialisation can have a "further deepening of a theme in the core, a new sub-discipline, or a specialist topic building on the core" (ECSA, 2014). Based on these outlines, cybersecurity knowledge can be seen as a specialisation, which is limited in the B.Eng degree due to the need to provide a substantial coherent core.

Therefore, there exists two main methods in which cybersecurity engineering can be formally introduced. The first would be a new undergraduate engineering program where a substantial part of the specialisation modules focus on cybersecurity and related topics, effectively requiring the registration of a new undergraduate course (ECSA, 2014). The second would be to introduce cybersecurity engineering at a postgraduate level by creating one or multiple modules specialising in cybersecurity and related topics. Considering these guidelines, this research favours the development of a cybersecurity postgraduate module for engineering graduates for specialisation in security.

4.2. Cybersecurity curricular guidelines

The ACM has recently developed the cybersecurity education curriculum framework (CSEC2017) as the first set of global curricular recommendations for cybersecurity education. This set of cybersecurity guidelines includes a discussion of the required conceptual knowledge and practical skills which will support the application of cybersecurity knowledge (Burley et al., 2017). The ACM suggests these curricular recommendations in the disciplines of computer science, computer engineering, information technology, information systems and security engineering. However, with the highly integrated computer systems used in the engineering discipline as a whole, these cybersecurity curricular guidelines can be applicable to the engineering field as a whole. The ACM recommends that a cybersecurity program should consist of five main components or dimensions, namely (Burley et al., 2017):

- **Foundational knowledge**: General education requirements already included in the engineering curricula. This includes the knowledge that should be included on top of the basic knowledge
- **Core Cybersecurity knowledge and skills**: Collectively represent the full cybersecurity body of knowledge: Data Security, Software Security, System Security, Human Security, Organisational Security and Societal Security.
- **Cross-cutting concepts**: Assist students in understanding the connections between the various knowledge areas. This includes concepts such as confidentiality, integrity, availability, risk and adversarial thinking.
- **Direct relationship to specialized/business domains**: A disciplinary lens which represents the underlying discipline which will form the foundation of the cybersecurity module, in this case, engineering.
- **Emphasis on soft skills**: Non-technical skills which includes teamwork, communication, accountability, conflict management and attention to detail.

The first three knowledge areas cover mostly technical work while the remaining three areas cover general computing and engineering topics relevant to cybersecurity. The CSEC2017 document suggests that all six knowledge areas should be covered in undergraduate cybersecurity programs. However, with the development of a postgraduate module it is suggested that a more narrowly focused approach should be taken by addressing the knowledge area most applicable to the work force needs. Initial focus on one knowledge area can be motivated as many knowledge areas are not mutually exclusive with concepts spanning over multiple knowledge areas.

It can be argued that the more general knowledge areas can be viewed as more applicable to a cybersecurity module for a postgraduate module in engineering. As not only computer or electronic engineering professionals will take this module, the inclusion of highly technical subject matter might not be the best choice. For an engineer studying towards a postgraduate degree and working in an engineering organisation, the aspects of organisational security will be of significant value. Therefore, Organisational Security would be considered as the most appropriate knowledge area for an initial module in cybersecurity. A brief breakdown of the

knowledge units included in the Organizational Security knowledge is shown in Table 1 (Burley et al., 2017).

Knowledge Units	Description
Security Policy and Governance	The internal and external operating environment of an organisation is addressed through policy and governance. SPG seeks to place constraints on the behaviour of its members.
Analytical Tools	Techniques and tools to recognize, block, divert, and respond to malicious activities; monitor and visualise network activities; manage detected suspicious activities.
Systems Administration	The configuration, operation, maintenance, and troubleshooting of technical system infrastructure.
Cybersecurity Planning	Defining the cybersecurity strategy of an organization and determining of required actions and resources.
Security Program Management	The application of knowledge, skills, tools, and techniques manage projects.
Personnel Security	Ensuring staff with a sound level of cybersecurity awareness.
Risk Management	Finding and controlling risks to organizational information assets.
Security Operations	Enhancing the security of the origin and traceability of sourced system components, such as externally produced hardware or software.

Table 1: Organisational Security (adapted from (Burley et al., 2017))

As ECSA specifies that specialisation must mainly happen on postgraduate level, this work discusses the creation of a postgraduate module focussing on Organizational Security. If the process of module development with this knowledge area is successful, other knowledge areas can be considered in future work.

4.3. Cybersecurity competencies

There often exists a mismatch between the competencies of graduates in STEM programs and the skills required by industry (Nair et al., 2009; Radcliffe, 2005; Wellington et al., 2002). A well-defined competency model can assist in the education, development and recruitment of professionals needed for a specific profession. Competencies are seen as critical to be a successful professional and to support the technical knowledge and skills obtained through studies. Due to the disconnect between graduate competencies and industry expectations, it is important to consider various competencies and skills as identified by cybersecurity professionals or relevant industries when developing a cybersecurity module (Burley et al., 2017). Therefore, the competencies defined for engineering in SA must be considered in the development of this module. ECSA prescribes required competencies in 11 exit level outcomes (ELOs) which are mandatory for all B.Eng graduates. The ELOs are described in Table 2.

No	Exit level outcome	Description
1	Problem solving	Identify, formulate, analyse and solve complex engineering problems creatively and innovatively.
2	Use of mathematics, natural sciences and engineering sciences	Apply knowledge of mathematics, natural sciences, engineering fundamentals and an engineering speciality to solve complex engineering problems.
3	Engineering Design and Synthesis	Perform creative, procedural and non-procedural design and synthesis of components, systems, works, products or processes
4	Investigation, Experiments and Data analysis	Demonstrate competence to design and conduct investigations and experiments
5	Engineering Methods, skills, tools & IT	Demonstrate competence to use appropriate engineering methods, skills and tools, including those based on information technology
6	Professional and General Communication	Demonstrate competence to communicate effectively, both orally and in writing, with engineering audiences and the community at large.
7	Impact of Engineering Activity	Demonstrate critical awareness of the sustainability and impact of engineering activity on the social, industrial and physical environment.
8	Team and multidisciplinary working	Demonstrate competence to work effectively as an individual, in teams and in multidisciplinary environments.
9	Lifelong (Independent) Learning	Demonstrate competence to engage in independent learning through well-developed learning skills.
10	Professional Ethics and Practice	Critical awareness of the need to act professionally and ethically, to exercise judgment and take responsibility within own limits of competence
11	Engineering Management	Demonstrate knowledge and understanding of engineering management principles and economic decision making

Table 2: ECSA exit level outcomes (adapted from (ECSA, 2014))

The rising demand for cybersecurity professionals in industry has also lead to industry calling for an agreed upon set of competencies which a cybersecurity professional must have. The various competencies deemed as important for cybersecurity engineers is captured in various cybersecurity competency models, which includes the National Initiative for Cybersecurity Education (NICE) and the US Department of Labour (DOL) Cybersecurity Competency model (Newhouse et al., 2017; University of Phoenix, 2015). The NICE Cybersecurity Workforce Framework (NCWF) describes cybersecurity competencies across various industries, organisations and job types. The framework states that cybersecurity professionals must be able to "adapt, design, develop, implement, maintain, measure and understand all aspects of cybersecurity". It provides a comprehensive reference of work roles, knowledge, skills and abilities required by cybersecurity professionals. The NCWF recognises that the cybersecurity workforce must not only be technically skilled, but must be able to apply cybersecurity knowledge to address challenges in the workplace (Newhouse et al., 2017).

The DOL Cybersecurity Competency Model builds on the NCWF to include specific competencies which cybersecurity professionals require. The model is a tiered pyramid, describing competencies for various levels of cybersecurity experts, ranging from entry level to expert (University of Phoenix, 2015). The model can be broadly divided into three clusters, namely foundational competencies, Industry related competencies and Occupational related competencies. Each cluster is further divided into 7 tiers. Considering the development of a general Cybersecurity Engineering module, focus will only be placed on the first 4 tiers represented in the model.

The first 3 tiers of the model represent the soft skills required by all individuals in the cybersecurity industry, while tier 4 includes more technical skills related to the cybersecurity industry. Competencies required for a B.Eng degree overlaps with the competencies included in the DOL Cybersecurity Competency Model. Table 3 lists the cybersecurity competencies as described by the DOL Cybersecurity Competency Model and indicates where it is included in the competencies defined by ECSA. By comparing the cybersecurity and engineering competencies, it can be determined which competencies are best to include in the cybersecurity module.

Tier	**Competency**	**ECSA ELO's**
1: Personnel effectiveness competencies	Interpersonal Skills & Teamwork	8
	Integrity	10
	Professionalism	10
	Initiative	1, 9
	Adaptability-Flexibility	1, 9
	Dependability-Reliability	9
	Lifelong Learning	9
2: Academic competencies	Reading	6
	Writing	6
	Mathematics	2
	Science	2
	Communication	2, 6
	Critical & Analytic Thinking	1, 2, 3, 5
	Fundamental IT User Skills	5
3: Workplace competencies	Teamwork	8
	Planning & Organizing	11
	Creative Thinking	3
	Problem Solving & Decision Making	1
	Working with Tools & Technology	5
	Business Fundamentals	11
4: Industry-wide technical competencies	Cybersecurity Technology	-
	Information Assurance	-
	Risk Management	7
	Incident Detection	-
	Incident Response and Remediation	-

Table 3: Mapping of competencies to ECSA exit level outcomes

From Table 3, it can be seen that all the Tier 1 to 3 competencies are adequately addressed in the current ELO's. However, Tier 4 competencies are not addressed in

the ELO's as they can be seen as more specialised, suggested by ECSA to be developed at postgraduate level. These competencies could therefore be a focus of the postgraduate module.

4.4. Actions for integrating cybersecurity knowledge

The drive to educate and train more cybersecurity professionals has led stakeholders to propose various actionable recommendations to higher education institutions. The following actions are included in the suggestion (University of Phoenix, 2015):

- **Ensure Alignment with Certifications:** Ensure quality and alignment of program by ensuring certification requirements are met.
- **Problem Based Learning (PBL**): Assess students' application of knowledge and skills, critical thinking, problem solving and teamwork skills through projects and practical case studies
- **Development of Competencies:** Provide students with opportunities to develop personal skills through project focused on real-world projects with technical and social aspects.
- **Promotion of Professional Ethics:** Place emphasis on professional ethics as cybersecurity experts often have access to and work with organisations' and customers' valuable data.

These suggested actions can be used in the development of the postgraduate module linking the knowledge areas and competencies to the classroom.

5. Basic outline of cybersecurity module for postgraduate engineering students

The CSEC2017 document (Burley et al., 2017) states that it should be used in collaboration with competencies defined through the competency frameworks. The cybersecurity competencies identified from the competency models can therefore be used to map to the knowledge units defined in the CSEC2017 guidelines. By integrating the proposed knowledge areas and the competencies, the module can be developed to suit the engineering industry's needs, and in future to expand the cybersecurity offerings in alignment with the requirements identified by industry.

Key Knowledge Units	Key Competencies	Key Actions
* Security Policy & Governance * Analytical Tools * Systems Administration * Cybersecurity Planning * Security Program Management * Personal Security * Risk Management * Security Operations	* Cybersecurity Technology * Information Assurance * Risk Management * Incident Detection * Incident Response and Remediation	* Alignment with Certifications * Problem Based Learning * Development of Competencies & Personal skills * Promotion of Professional Ethics

Table 4: Layout for cybersecurity module for postgraduate engineering

The key knowledge units included in Table 4 relates to the knowledge units identified for Organisational Security in Section 4.2. Topics included in these knowledge units are knowledge on privacy, law and ethics relating to cybersecurity, using tools to secure technical system infrastructure, defining of cybersecurity strategies and managing of cybersecurity risks within an organisation. In such a highly integrated working environment of social and technical systems, the essential duties and responsibilities of cybersecurity engineering professionals include activities such as developing, managing and enforcing security strategies and policies within company guidelines and supporting incident response activities to mitigate damage, determine impact, and implement corrective actions. In addition, companies require cybersecurity engineers to adequately assist organisations in risks associated with information security in projects and assessing new security technologies and recommends possible implementation strategies. An engineer with a clear understanding of how security can be integrated on an administrative, strategic, operational, technical and social level, will greatly benefit the organisation.

The key competencies listed in Table 4 covers the Tier 4 competencies identified from the DOL Cybersecurity Competency Model discussed in Table 3 which are not addressed by the ELO's in undergraduate engineering. The inclusion of these competencies therefore ensures that the first four competency tiers defined for cybersecurity professionals are covered in undergraduate study and this particular postgraduate study, complementing the undergraduate engineering competencies covered at undergraduate level.

The key actions included in Table 4, discussed in Section 4.4, are included to ensure that the postgraduate model successfully link the identified knowledge units and competencies to the classroom. These actions must be taken into account with the design of the postgraduate module to ensure that the student who successfully complete this program has the necessary cybersecurity knowledge and skills which are required by industry. Through the integration of project based learning, the module can make use of relevant case studies or projects in the field of cybersecurity for teaching and assessments of the required skills and knowledge.

6. Conclusion

This paper described the process followed for the development of a postgraduate module in cybersecurity engineering. The Qualification Standard for Bachelor of Engineering (B.Eng) stipulates that undergraduate engineering programs should provide a sound foundation where postgraduate programs must support specialisation. The development of a postgraduate module speaks to this recommendation to provide engineers with cybersecurity knowledge at postgraduate level. The basic outline of a cybersecurity module for postgraduate engineering students is developed and presented in this paper. The key aspects contained in this outline can guide universities in the development of a postgraduate module in cybersecurity. This work will contribute to cybersecurity curriculum design in engineering which could provide a roadmap/framework for the integration of cybersecurity into formal engineering education.

Future research would include the utilisation of the basic outline presented in this paper to construct a clear module outline by matching the selected knowledge units to the competencies. The key actions included in the outline must be used in the design of the module outline as the mechanism for linking the knowledge areas to the cybersecurity competencies.

7. References

BMBF, B. für B. und F., 2011. Industrie 4.0 [WWW Document] (2011) URL https://www.bmbf.de/de/zukunftsprojekt-industrie-4-0-848.html (accessed 8.20.17).

Burley, D.L., Bishop, M., Buck, S., Futcher, L., Gibson, C.D., Hawthorne, E., Kaza, S., Levy, Y., Mattord, H., Parrish, A. (2017). Cybersecurity Curricula 2017.

Cisco Advisory Services, 2015. Mitigating the cybersecurity skills shortage.

Dilger, D.E. (2017). Ten Years of iPhone: the past present and future of Apple ’s blockbuster phenomenon [WWW Document]. URL http://appleinsider.com/articles/17/01/09/ten-years-of-iphone-the-past-present-and-future-of-apples-blockbuster-phenomenon- (accessed 8.10.17).

ECSA, E.C. of S.A. (2014). Qualification Standard for Bachelor of Science in Engineering (BSc (Eng))/ Bachelors of Engineering (BEng): NQF Level 8 4, 1–10.

Fripp, C., 2017. South Africa simply doesn ’ t have enough cybersecurity experts. HTXT.Africa 3–5.

Frost and Sullivan (2015). The 2015 $(ISC)^2$ Global Information Security Workforce Study. A Frost Sullivan White Pap. 1–28.

Gardner, D. (2016). Capgemini and HPE Team Up to Foster Behavioral Change That Brings Better Cyber Security Across Application Lifecycles [WWW Document]. URL http://www.briefingsdirecttranscriptsblogs.com/2016/04/capgemini-and-hpe-team-up-to-foster.html (accessed 9.1.17).

Hermann, M., Pentek, T., Otto, B. (2016). Design principles for industrie 4.0 scenarios. Proc. Annu. Hawaii Int. Conf. Syst. Sci. 2016–March, 3928–3937. doi:10.1109/HICSS.2016.488

McGettrick, A. (2013). Toward curricular guidelines for cybersecurity, Report of a Workshop on Cybersecurity Education and Training. doi:10.1145/2538862.2538990

Morgan, S., 2015. IBM's CEO On Hackers: "Cyber Crime Is The Greatest Threat To Every Company In The World" [WWW Document]. URL https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#1baf053373f0 (accessed 9.1.17).

Nair, C., Patil, A., Mertova, P. (2009). Re-engineering graduate skills: a case study. Eur. J. Eng. Educ. 34, 131–139.

Newhouse, W., Keith, S., Scribner, B., Witte, G., 2017. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. doi:10.6028/NIST.SP.800-181

Nordrum, A. (2016). Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated [WWW Document]. IEEE Spectr. URL https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated (accessed 9.4.17).

Radcliffe, D.F. (2005). Innovation as a meta attribute for graduate engineers. Int. J. Eng. Educ. 21, 194–199.

Tamura, E. (2017). Hewlett Packard Enterprise Leads Transformation of Cyber Defense with "Build it In" and "Stop it Now" Approach [WWW Document]. Press Release. URL http://www8.hp.com/us/en/hp-news/press-release.html?id=2184147#.Wa0HOLIjG00 (accessed 9.3.17).

University of Phoenix (2015). Competency Models for Enterprise Security and Cybersecurity Research.

University of San Diego (2016). Why Cyber Security Engineers Will Soon Be in High Demand.

Wellington, P., Thomas, I., Powell, I., Clarke, B. (2002). Authentic assessment applied to engineering and business undergraduate consulting teams. Int. J. Eng. Educ. 18, 168–179.

Zephoria (2017). The Top 20 Valuable Facebook Statistics [WWW Document]. Zephoria Digit. Mark. URL https://zephoria.com/top-15-valuable-facebook-statistics/ (accessed 8.20.17).