A Case Study of a Cybersecurity Programme

Curriculum Design, Resource Management, and Reflections

Muhammad Rizwan Asghar
The University of Auckland
New Zealand
r.asghar@auckland.ac.nz

Andrew Luxton-Reilly
The University of Auckland
New Zealand
a.luxton-reilly@auckland.ac.nz

ABSTRACT

Cybersecurity is an area of growing international importance. In response to global shortages of Cybersecurity skills, many universities have introduced degree programmes in Cybersecurity. These programmes aim to prepare students to become Cybersecurity practitioners with advanced skills in a timely manner. Several universities offer Cybersecurity degrees, but these have been developed ad hoc, as there is currently no internationally accepted Cybersecurity curriculum.

Recently, an ITiCSE working group on global perspectives on Cybersecurity education developed a competency-based framework that aims to help institutions to implement Cybersecurity programmes. In this report, we present a case study of a Cybersecurity programme at the University of Auckland. We discuss how the curriculum and resource management of this programme evolved, and we present some challenges for the design and delivery of a Cybersecurity programme in the light of this competency-based framework.

KEYWORDS

Cybersecurity education, Cybersecurity curriculum

ACM Reference Format:
Muhammad Rizwan Asghar and Andrew Luxton-Reilly. 2020. A Case Study of a Cybersecurity Programme: Curriculum Design, Resource Management, and Reflections. In *The 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20), March 11–14, 2020, Portland, OR, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Cybersecurity is a recent and highly-demanding discipline that did not exist a decade ago. To address the global shortage of Cybersecurity skills [4], many universities have introduced degree programmes in Cybersecurity. These programmes aim at preparing Cybersecurity practitioners with advanced skills in a timely manner, which may take years to experience to acquire in the workforce.

Although various curriculum initiatives are working towards curriculum guidelines for Cybersecurity [7], there is no established global Cybersecurity curriculum currently followed by universities. There is a genuine need to support educators who are designing and offering new Cybersecurity degree programmes. To this end, an ITiCSE working group on global perspectives on Cybersecurity education has recently developed a competency-based framework to help in the design and implementation of Cybersecurity programmes [9].

In this report, we present a case study of the design and implementation of a Cybersecurity Master's programme at an urban university. We discuss how this programme was initiated and evolved in terms of curriculum development and resource management. We also illustrate how the competency-based framework for Cybersecurity may be used in conjunction with institutional frameworks for describing graduate capabilities.

2 RELATED WORK

As the demand for courses involving Cybersecurity has increased, we have seen an increase in the literature on teaching and learning of Cybersecurity, including descriptions of how Cybersecurity topics may be introduced in high schools [6], environments for teaching Cybersecurity [20], and activities that aim to make university Cybersecurity curriculum more engaging using games [18, 19] or adversarial competitions [1]. These case studies help to disseminate examples of engaging teaching that could be adapted for use in the classroom, and work to build a community capable of delivering Cybersecurity programs, as recommended by Siraj et al. [12].

However, in addition to reports on innovative delivery, the community benefits from case studies of overall course structure, curriculum, and programme design. Hoag [5] provides one such case study in a report on the iterative development of a Cybersecurity curriculum. Initially, a major in Computer Networking and Information Security was offered, but not long afterwards the programme was enhanced with a specialisation in Cybersecurity adding courses in Information Assurance policy and Digital Forensics. The curriculum was further revised to provide students with flexibility, and the National Cybersecurity Workforce Framework developed by the National Initiative for Cybersecurity Education (NICE) was used to guide the discussion of curriculum revisions.

More recently, Kim and Beuran [8] describe a high-level approach to designing a Cybersecurity programme that considers three dimensions: institutional, users, and external factors. The authors report that they were in the process of developing a Master program, but at the time of publication had not completed the process.

Several other multi-national collaborations have offered guidance for Cybersecurity curricula. An early ITiCSE working group focusing on Information Assurance curricula in 2009 laid the foundation for later developments [3] by describing the state of the

SIGCSE '20, March 11–14, 2020, Portland, OR, USA
© 2020 Association for Computing Machinery.
ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

field at that time. A subsequent working group the following year proposed a set of topic areas that would form the Body of Knowledge (BoK) for future Information Assurance education [2]. A third working group in 2011 studying the implementation of Information Assurance programmes offered in two- and four-year institutions found that there was little consistency between programmes and suggested that curricula guidelines would help to develop coherence in the discipline [10]. Subsequent model curricula continued to include topics on Information Assurance and Security as part of a more traditional Information Technology curriculum [11]. However, a document proposing guidelines for Cybersecurity education programmes by *The Joint Task Force on Cybersecurity Education (JTF)* was released in 2017 [7]. A recent ITiCSE working group provides an excellent overview of global Cybersecurity frameworks and curricula [9].

Despite several frameworks and curricula documents, there remain very few published case studies of degree programmes that address Cybersecurity. To the best of our knowledge, there are no previous case studies that report on Master's programmes offering Cybersecurity education.

3 CYBERSECURITY DEGREE PROGRAMME: AN OVERVIEW

The Master of Cybersecurity programme was established to produce graduates with an advanced security skill set suitable for professional work. The programme aims to develop a pool of graduates capable of supporting industry and government needs for Cybersecurity management in the business domain. Students completing the programme should acquire security knowledge and skills that would normally require years of work in the field to acquire.

The design of the programme leveraged institutional strengths in Computer Science, Information Systems and Operations Management, and Software Engineering to offer security professionals a specific skill set. System administrators, programmers, software developers, business unit and supply chain managers, and a host of other mid-tier management could all potentially benefit from the programme to further improve their career opportunities. In New Zealand, a year of full-time study at University normally consists of 120 credit points (hereafter referred to as points). This taught programme requires 120 points of postgraduate study, which can be completed with one year of full-time study, or can take up to four years with part-time study. The programme comprises six courses (15 points each) and a dissertation (30 points). The six taught courses involve typical delivery methods such as lectures, seminars, tutorials, and labs, while the dissertation is completed under appropriate supervision from an expert in Cybersecurity. The programme has three main components.

- **The first component (60 points)** integrates system security and security management. In this component, students will develop a deep understanding of security mechanisms and how to apply them for protecting resources such as network infrastructures and data, and how to translate high-level policies and regulations into concrete mechanisms to manage security infrastructures. These compulsory courses in Computer Science and Information Systems ensure that students will have well-rounded skills and knowledge of techniques required for business infrastructure security.
- **The second component (30 points)** enables the development of particular specialist strengths alongside the core knowledge, such as entrepreneurial and business skills, or further depth in Information Systems or Computer Science. The 30 points of elective courses allow students to develop particular specialist strengths alongside the core knowledge, such as Operations Management or Computer Systems, or further depth in Computer Science or Information Systems as needed.
- **The third component of the programme (30 points)** requires students to apply and deepen their skill set in a research project under supervision by an academic and/or practitioner from industry.

3.1 Programme Courses

The programme comprises four compulsory taught courses (60 points), and ten taught elective courses from which a student is expected to choose two courses (30 points). The program also requires the student to complete a dissertation (30 points). There is one compulsory course from Information Systems (IS) and three courses from Computer Science (CS). These compulsory courses are:

- IS727: Information Security
- CS725: System Security
- CS726: Network Security
- CS727: Cryptographic Systems

The elective courses are as follows:

- CS702: Smartphone Security
- CS705: Human Computer Interaction (HCI)
- CS720: Advanced Analysis of Algorithm
- CS732: Software Tools and Techniques
- CS742: Data Communications
- IS720: Information Systems Research
- IS730: Telecommunications Management
- IS737: Enterprise Systems
- IS750: Research Methodology – Quantitative
- IS751: Research Methodology – Qualitative

Our programme courses cover how to design, plan, and manage a secure Information Technology (IT) infrastructure. Basically, a student can develop a specialised combination of skills that include computer science, information systems, software engineering and operations management. Graduates of the programme develop their expertise in:

- Authentication and access control
- Governance, information assurance, and risk analysis
- Network infrastructure and protocol
- Physical security and surveillance
- Research skills

To know more about courses and topics covered under the programme, an interested reader is referred to [14].

3.2 Graduate Profile

The University of Auckland, which is a research-led comprehensive university, uses a 3-level framework [15] to describe the profile of graduates from the university [13].

- **Level 1 (Aspirations)** captures the University's overarching strategic aspirations for our graduates. This level describes the aspirational profile of graduates as scholars, innovators, leaders and global citizens.
- **Level 2 (Themes)** covers generic capabilities that the university seek to foster in all graduates through the teaching and learning experiences of their programmes. These capabilities are divided into 6 interrelated domains or themes including:
  1. *Disciplinary Knowledge and Practice*
  2. *Critical Thinking*
  3. *Solution Seeking*
  4. *Communication and Engagement*
  5. *Integrity and Independence*
  6. *Social and Environment Responsibilities.*
- **Level 3 (Capabilities)** embeds knowledge, skills, abilities, and values that comprise each of the themes. This level deals with a set of qualification specific capabilities in order to provide an embedded graduate profile, which refers to the way that each qualification interprets and delivers the themes.

Although the Aspirations and Themes are common to all students, the Capabilities are intended to be embedded within each programme so cannot be described more generally. These capabilities that comprise the third level of the graduate profile are described at a similar level to the competency-based framework proposed by Parrish et al. [9] for Cybersecurity programmes. In addition to achieving the generic graduate profile, those who complete this programme will have the following capabilities:

- an understanding of the current theoretical and practical developments in Cybersecurity management drawing on information systems, computer science, and business domains
- ability to assemble and implement applied security technologies and tools
- ability to integrate strategies for managing digital security with business practice, and to establish governance policies for rapid incident response
- problem solving and high-levels of critical analysis
- organisation and time management skills, and
- effective visualisation and communication skills.

To better inform students about the relationship between courses and program outcomes, we map graduate capabilities with learning outcomes of individual courses.

4 PROGRAMME INTRODUCTION AND INSTITUTIONAL REQUIREMENTS

In this section, we reflect on the process involved in the introduction of a new programme and institutional factors that may impact on the design of that programme.

4.1 Programme Proposal

Depending on the institution and accrediting body, the introduction of a new programme may need a business case to be prepared, or a proposal that justifies the need, and feasibility, for the programme. A proposal that advocates for the value of a Cybersecurity programme should highlight the need for secure infrastructure in public and private sectors (*e.g.,* banking and finance, transportation, medical, education and government) within and outside the region of interest.

To emphasise the importance of Cybersecurity it may be useful to discuss the potential damage inflicted on individuals and organisations by cyberattacks and how Cybersecurity professionals can mitigate the potential risk and resolve issues as they arise. It may also be valuable to engage with industry experts who have an interest in both accessing the talent pool that would be created from the programme and supporting (and potentially participating in) the proposed programme themselves.

Other aspects that may be considered include how the programme:

- aligns with the University's long-term strategies;
- leverages the University's strength in different academic units and/or staff;
- results in synergistic relationships between the teaching programmes of academic units in order to incorporate interdisciplinary aspects of Cybersecurity such as including technical, management, and business components; and
- cover knowledge areas that are relevant to industry.

Consequently, the selection of teaching expertise and courses should meet the needs of the relevant stakeholders. Ideally, such programs should be a collaborative endeavour that involves input from industry, perhaps in the form of guest lectures and shared supervision.

4.2 Planning and Management

New programmes, particularly if they are popular, may require additional institutional support in the form of administrative and teaching support, and possibly teaching laboratories. Projecting the growth of student enrolments plays an important role in the planning process for such programmes.

Based on our experience, we suggest that it is more pragmatic to introduce the programme courses progressively. That is, instead of introducing all the courses in the first semester or first year, new courses could be offered as the programme matures. In our experience, introducing the programme with limited additional resources was demanding. In particular, the start of the programme required substantial changes to our existing courses to make them fit for our programme. One major challenge was to minimise potential overlap between existing and new courses as we progressively broadened the coverage of the programme to incorporate a diverse range of Cybersecurity topics. As expected, the first few years of the programme involve a high workload as new courses are developed, so additional support should be provided if possible during early stages.

4.3 Entry Requirements and Completions

The entry requirements for the Master's programme include the completion of one of the following:

- A four-year bachelors degree or
- An honours degree (*i.e.,* a one-year postgraduate degree) or
- A bachelors degree and a one-year professional qualification, or three years of professional experience in Cybersecurity or related areas.

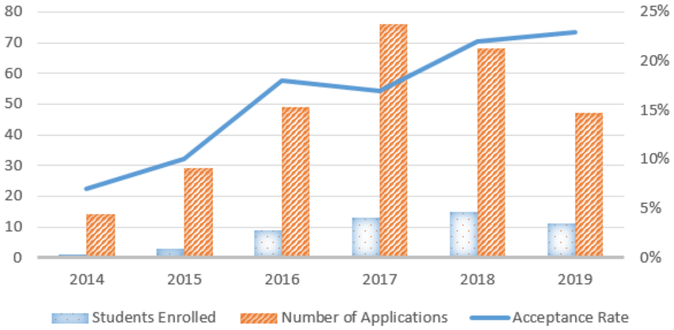

Figure 1: Acceptance rate of our Master of Cybersecurity programme based on the number of students enrolled and the number of applications processed.

The degree used to meet the entry requirements should be in a "relevant discipline" but is not required to be a cognate programme (*i.e.,* a Computer Science or Software Engineering programme). This enables candidates with a wide range of background to apply for the programme, but this also makes it difficult to decide who is a suitable candidate. To address this concern, the admission office receives all the applications and makes initial checks such as general requirements including language and admission requirements. Next, the application is forwarded to the Cybersecurity programme coordinator who makes a decision based on whether the candidate has sufficient background knowledge to attempt the courses that comprise the programme. As illustrated in Figure 1, the quality of applicants has been steadily increasing, resulting in the acceptance rate improving from 7% in 2014 to 23% in 2019. The admission criteria is strict in order to minimise the challenges that non-technical students can face otherwise.

Table 1 lists the numbers of students, as well as the total enrollments listed as Equivalent Full-Time Students (EFTS) and the percentage of completions. Given the domestic and global demands for Cybersecurity, the steady rise of applicants and actual enrolments, it is likely that EFTS will continue to rise further. Completion numbers are as expected since the number of full-time students is small in comparison to part-time students who aim to complete in either two or four years. So far, three students have discontinued their studies.

5 QUALITY ASSURANCE

5.1 Accreditation

Universities New Zealand [17] is a statutory body with the authority for the quality assurance of academic programs delivered in New Zealand universities. Universities New Zealand delegates responsibility for accreditation of academic programs to the Committee on University Academic Programs (CUAP) [16], which review the introduction of new programs, changes to existing programs, and the broad descriptions of courses that comprise the program. Individual universities take responsibility for the quality assurance of courses delivered at that University.

5.2 Quality Assurance of Courses

The programme courses conform to the University's examination regulations and Faculty standards at the postgraduate level. Assessments, including examination, tests, and assignments/projects as well as student performance are evaluated internally and moderated externally every semester by an appropriate assessor. Students are already assessed upon applying for the programme, which helps in identifying the gaps of the students and the requirements for catch-up courses. The assessment results provided are similar to other disciplines in terms of grade distribution. The course assessments, evaluations, and student performance meet the level and goals of the programme, and indicate high quality postgraduate teaching.

The course review documents are prepared at the end of each semester in order to report changes implemented and plan for further improvements. This course review practice not only helps in improving the quality of this programme's courses but also creates a great sharing environment for teaching staff to reflect on what worked well and what could be improved.

5.3 Supervision of Dissertations

The overall performance of the graduates is satisfactory, with an average grade of B in the degree programme. The experience of supervising dissertation students in the programme is diverse.

Some students chose to start their dissertation in their first semester before they had completed any taught courses. However, the majority of these students lacked research skills and performed poorly in the dissertation. Students who completed taught courses before enrolling in the dissertation performed at a higher level since the taught courses are research-informed and typically require students to engage in smaller research projects throughout the course assessments.

Nevertheless, some graduates show a strong interest in research and development, and their dissertations are of high quality. Several dissertations resulting from the programme have been developed into articles published at high-quality peer-reviewed international venues.

5.4 Pedagogical Practices and Inclusiveness

The pedagogical practices adopted by the staff teaching the programme are diverse, but frequently involve active learning approaches. For example, in one course, a constructivist teaching strategy facilitates a Cybersecurity attacker and a Cybersecurity defender, thus using competitive peer evaluation strategies in teaching Cybersecurity. Students appear to appreciate such active learning approaches.

In most of our course (*e.g.,* CS702 and CS726), we have group projects so that students can team up, discuss, and work on the final report. In some courses, such as CS702, there can be up to 5

Table 1: Summary information on enrolments and completions of the Master of Cybersecurity programme (Information obtained as of the 12 March 2019).

Academic Year	New Students	Returning Students	Full-time Students	Part-time Students	Total EFTS	Completing Students	% Completions	Discontinuing Students	% Discontinuation
2014	1	0	0	1	0.250	1	100%	0	0%
2015	2	1	0	3	1.000	1	50%	1	50%
2016	7	2	2	7	5.375	6	86%	1	14%
2017	8	5	0	13	4.625	2	25%	0	0%
2018	12	3	6	9	10.167	5	42%	1	8%
2019	4	8	3	9	5.250	0	0%	0	0%

Academic Year is when the student enrolled.
New Students are those who enrol for the very first time in that academic year.
Returning Students are those who continue the programme in that academic year.
Full-time Students are those who take 100 points or more over in an enrolment year.
Part-time Students are those who take fewer than 100 points in an enrolment year.
Total EFTS (Equivalent Full-Time Student) is the combined total of new and returning EFTS.
Completing Students are those who eventually complete and meet the requirements for the programme.
Discontinuing Students are those who eventually discontinued the programme.

group members. Given a diverse set of skills and background of students, there are different opportunities (including development phase, challenge phase, final report, project presentation) how each student can contribute to CS702 projects. That is, students can work on different tasks yet they are expected to contribute equally. The project grade is based on the overall percentage contribution of each group member.

6 PROGRAMME EVALUATION

6.1 Graduating Year Review

The Graduating Year Review (GYR) process is a quality assurance and improvement process for new programmes at our University. The process determines whether (i) a programme is meeting expectations; (ii) there are any significant problems; (iii) priorities for improvement and how these will be achieved; and (iv) the programme is viable. In this section, we report on the data sources and evaluation process for the programme.

The GYR process expects a portfolio of information relating to the programme. This portfolio is accompanied by an evaluation report related to the purpose and justification of the programme, which is prepared by the GYR Departmental Chair. The report is supported by the original proposal establishing the programme, relevant department handbooks, website description, course outlines, course descriptions, course reviews, examination papers, reports of external assessors, sample dissertations, examiner reports, students' successes, teaching evaluations, statistical information on enrolments, completions, pass rates and grade distribution, and how any feedback was addressed. The evaluation report and the support material are sent to an independent review panel.

6.2 Programme Achievement and Acceptability

The panel review and external assessor reports provide evidence that the stated goals of the programme have been achieved. The stated goal of the programme is to develop a pool of talented graduates capable of helping to address the large industry and government demand for skilled Cybersecurity professionals. The review panel report concluded that the Master of Cybersecurity programme is meeting its goal. Our graduates secured technical and leading positions in security management in New Zealand and abroad.

An increasing interest in applicants and enrolments is an indication of the programme's acceptability to students. Quantitatively, around 85% of student report that they are "satisfied" or "very satisfied" with the quality of the courses comprising the programme. Qualitatively, the feedback from students has been very positive in terms of the curriculum, teaching, learning, assessments, guidance, and resources.

The quality of teaching is assured by regular monitoring and by the selection of lecturers who are research active, and passionate about the subjects they teach. Academic course work and research are complemented by guest lectures from industry. The student cohort is diverse: while part-time students dominate, there are also several full-time students; there is a balance between students that are new to the University of Auckland and those that are returning; and there is a growing body of international students (mostly from Asia and India).

The achievement of the graduate attributes is regularly checked in the assessment processes. The results of examination, assessment and regular evaluations of courses since the inception of the programme continue to indicate positive achievement of the graduate profile.

The review panel was unanimous in its agreement that the programme is fulfilling its purpose and achieving the stated goals in the original proposal. The panel agrees that: course materials are appropriate and the curriculum design is coherent; teaching, learning and assessment approach is appropriate; and student support and guidance, resources, and student feedback mechanisms are also appropriate. The review panel reported that the students have enough flexibility in the programme and its graduates have been well received by industry.

Table 2: Mapping our programme to the Cybersecurity competency-based framework.

	Compulsory Courses				*Elective Courses*	
Cybersecurity Domains	**IS727**	**CS725**	**CS726**	**CS727**	**CS702**	...
Governance	Policy, Strategy, Compliance, & Standardisation	Policy, Compliance, & Standardisation	Policy & Standardisation	Policy, Strategy, Compliance, & Standardisation	Policy, Strategy, Compliance, & Standardisation	
Risk Management	Threat Modelling, Asset Evaluation, Mitigation, & Vulnerability	Threat Modelling, Mitigation, & Vulnerability	Threat Modelling, Mitigation, & Vulnerability	Threat Modelling, Mitigation, & Vulnerability	Threat Modelling, Mitigation, & Vulnerability	
Constraints	Legal, Ethical, Organisational, Privacy, & Political	Legal, Ethical, Organisational, & Privacy	Legal, Ethical, Organisational, & Privacy	Organisational & Privacy	Legal, Ethical, Organisational, & Privacy	
Controls	Administrative, Physical, & Technical	Administrative & Technical	Administrative, Physical, & Technical	Technical	Administrative, Physical, & Technical	

The programme courses include IS727 (Information Security), CS725 (System Security), CS726 (Network Security), CS727 (Cryptographic Systems), CS702 (Smartphone Security), and other courses on HCI, Data Communications, and Information Systems.

7 MAPPING TO CYBERSECURITY EDUCATION FRAMEWORK

The ITiCSE 2018 working group on Cybersecurity education proposed a Cybersecurity education framework, and emphasises adversarial aspects as a unifying basis for Cybersecurity [9]. Given the interdisciplinary nature of Cybersecurity, the report describes specific security disciplines along with competency levels.

As a framework for Cybersecurity education, the report presents two overall approaches. The first approach is to augment existing computing courses with Cybersecurity topics. The second approach suggests developing brand new standalone Cybersecurity programmes. In our Master of Cybersecurity programme, we neither completely relied on augmenting existing courses nor developed a new standalone programme. Instead, we used a combination of revising existing courses to include new Cybersecurity topics, and introducing completely new courses.

The report also presents a competency-based framework for futuristic Cybersecurity education [9], where competency represents knowledge, technical skills, and human disposition. We believe that this futuristic model maps well to the University of Auckland new graduate profile framework, where Level 3 can be considered to incorporate competencies.

Table 2 shows a mapping of our programme to the Cybersecurity competency-based framework [9]. There are four main Cybersecurity domains including *Governance*, *Risk Management*, *Constraints*, and *Controls*. The report describes competencies for each Cybersecurity domain as follows:

Governance:
Policy, *Strategy*, *Compliance*, and *Standardisation*.

Risk Management:
Threat Modelling, *Asset Evaluation*, *Mitigation*, and *Vulnerability*.

Constraints:
Legal, *Ethical*, *Organisational*, *Privacy*, and *Political*.

Controls:
Administrative, *Physical*, and *Technical*.

Due to space limitations, we focus on compulsory core courses and the competencies covered by those courses. We also provide an example of a single elective course as shown in Table 2. Note that each course is expected to demonstrate a subset of, if not all, graduate capabilities. These graduate capabilities are linked to course learning outcomes. Some of our programme courses demonstrate all graduate capabilities (*e.g.,* CS726 and CS702). The programme also covers adversarial aspects of Cybersecurity in some courses by facilitating both attackers and defenders in group projects (*e.g.,* [1]).

8 CONCLUSIONS

In this work, we presented a case study of a Cybersecurity programme. We briefly provided an overview of our programme and graduate profile framework. We reflected on the process involved in the introduction of our programme and some institutional factors regarding its design. We also discussed programme evaluation and quality assurance aspects. Further, we mapped this programme to the Cybersecurity education framework and the corresponding competency-based framework proposed by the ITiCSE working group on Cybersecurity education. We believe that this work might assist educators in understanding the whole lifecycle of new Cybersecuirty curriculum. The insights might be helpful for those who are planning to offer a new degree programme in Cybersecurity.

REFERENCES

[1] Muhammad Rizwan Asghar and Andrew Luxton-Reilly. 2018. Teaching Cyber Security Using Competitive Software Obfuscation and Reverse Engineering Activities. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE '18)*. ACM, New York, NY, USA, 179–184. https://doi.org/10.1145/3159450.3159489

[2] Stephen Cooper, Christine Nickell, Lance C. Pérez, Brenda Oldfield, Joel Brynielsson, Asim Gencer Gökce, Elizabeth K. Hawthorne, Karl J. Klee, Andrea Lawrence, and Susanne Wetzel. 2010. Towards Information Assurance (IA) Curricular Guidelines. In *Proceedings of the 2010 ITiCSE Working Group Reports (ITiCSE-WGR '10)*. ACM, New York, NY, USA, 49–64. https://doi.org/10.1145/1971681.1971686

[3] Stephen Cooper, Christine Nickell, Victor Piotrowski, Brenda Oldfield, Ali Abdallah, Matt Bishop, Bill Caelli, Melissa Dark, Elizabeth K Hawthorne, Lance Hoffman, et al. 2010. An exploration of the current state of information assurance education. *ACM SIGCSE Bulletin* 41, 4 (2010), 109–125.

[4] Adam P Henry. 2017. *Mastering the cyber security skills crisis: realigning educational outcomes to industry requirements*. Technical Report. ACCS Discussion paper.

[5] Jim Hoag. 2013. Evolution of a Cybersecurity Curriculum. In *Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference (InfoSecCD '13)*. ACM, New York, NY, USA, Article 94, 6 pages. https://doi.org/10.1145/2528908.2528925

[6] Ge Jin, Manghui Tu, Tae-Hoon Kim, Justin Heffron, and Jonathan White. 2018. Game Based Cybersecurity Training for High School Students. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE '18)*. ACM, New York, NY, USA, 68–73. https://doi.org/10.1145/3159450.3159591

[7] Joint Task Force on Cybersecurity Education. 2017. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity.

[8] Eunyoung Kim and Razvan Beuran. 2018. On Designing a Cybersecurity Educational Program for Higher Education. In *Proceedings of the 10th International Conference on Education Technology and Computers (ICETC '18)*. ACM, New York, NY, USA, 195–200. https://doi.org/10.1145/3290511.3290524

[9] Allen Parrish, John Impagliazzo, Rajendra K. Raj, Henrique Santos, Muhammad Rizwan Asghar, Audun Jøsang, Teresa Pereira, and Eliana Stavrou. 2018. Global Perspectives on Cybersecurity Education for 2030: A Case for a Meta-discipline. In *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018 Companion)*. ACM, New York, NY, USA, 36–54. https://doi.org/10.1145/3293881.3295778

[10] Lance C. Pérez, Stephen Cooper, Elizabeth K. Hawthorne, Susanne Wetzel, Joel Brynielsson, Asim Gencer Gökce, John Impagliazzo, Youry Khmelevsky, Karl Klee, Margaret Leary, Amelia Philips, Norbert Pohlmann, Blair Taylor, and Shambhu Upadhyaya. 2011. Information Assurance Education in Two- and Four-year Institutions. In *Proceedings of the 16th Annual Conference Reports on Innovation and Technology in Computer Science Education - Working Group Reports (ITiCSE-WGR '11)*. ACM, New York, NY, USA, 39–53. https://doi.org/10.1145/2078856.2078860

[11] Mihaela Sabin, H Alrumaih, B Lunt, M Zhang, B Byers, W Newhouse, B Paterson, S Peltsverger, C Tang, G van der Veer, et al. 2017. *Curriculum Guidelines for Baccalaureate Degree Programs in Information Technology*. Technical Report. Technical Report, Association of Computing Machinery, New York, NY, USA.

[12] Ambareen Siraj, Blair Taylor, Siddarth Kaza, and Sheikh Ghafoor. 2015. Integrating Security in the Computer Science Curriculum. *ACM Inroads* 6, 2 (May 2015), 77–81. https://doi.org/10.1145/2766457

[13] The University of Auckland. 2019. Graduate Profile. https://www.auckland.ac.nz/en/students/forms-policies-and-guidelines/student-policies-and-guidelines/graduate-profile.html

[14] The University of Auckland. 2019. Postgraduate study in Digital Security. https://www.auckland.ac.nz/en/study/study-options/find-a-study-option/digital-security/postgraduate.html

[15] The University of Auckland. 2019. Three Levels of the Graduate Profile. https://cdn.auckland.ac.nz/assets/auckland/students/forms-policies-and-guidelines/student-policies-and-guidelines/graduate-profile/graduate-profile-visual-overview-of-3-levels.pdf

[16] Universities New Zealand. 2019. Committee on University Academic Programmes (CUAP). https://www.universitiesnz.ac.nz/about-universities-new-zealand/unz-committees-and-working-groups/committee-university-academic

[17] Universities New Zealand. 2019. Universities New Zealand. https://www.universitiesnz.ac.nz

[18] Valdemar Švábenský, Jan Vykopal, Milan Cermak, and Martin Laštovička. 2018. Enhancing Cybersecurity Skills by Creating Serious Games. In *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018)*. ACM, New York, NY, USA, 194–199. https://doi.org/10.1145/3197091.3197123

[19] Richard Weiss, Michael Locasto, Jens Mache, and Vincent Nestler. 2013. Teaching Cybersecurity Through Games: A Cloud-based Approach. *J. Comput. Sci. Coll.* 29, 1 (Oct. 2013), 113–115. http://dl.acm.org/citation.cfm?id=2527148.2527175

[20] Dongqing Yuan. 2017. Developing a Hands-on Cybersecurity Laboratory with Virtualization. *J. Comput. Sci. Coll.* 32, 5 (May 2017), 118–124. http://dl.acm.org/citation.cfm?id=3069621.3069649