Chapter 4

Cyber Security Body of Knowledge and Curricula Development

Evon M Abu-Taieh, Auhood Abd. Al Faries, Shaha T. Alotaibi and Ghadah Aldehim

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.77975

Abstract

The cyber world is an ever-changing world and cyber security is most important and touches the lives of everyone on the cyber world including researchers, students, businesses, academia, and novice user. The chapter suggests a body of knowledge that incorporates the view of academia as well as practitioners. This research attempts to put basic step and a framework for cyber security body of knowledge and to allow practitioners and academicians to face the problem of lack of standardization. Furthermore, the chapter attempts to bridge the gap between the different audiences. The gap is so broad that the term of cyber security is not agreed upon even in spelling. The suggested body of knowledge may not be perfect, yet it is a step forward.

Keywords: body of knowledge, cyber security, ciphering, compression, database, operating systems, computer network

1. Introduction

Cyber security is a newly developed concept, proving to be of significance in the cyber world. The concept of cyber security admitted by many is not clear hence not standardized. This chapter aims to suggest a body of knowledge (BOK) based on two aspects: practitioners and academia. The chapter studied previous work of ACM, NICE, NICCS, and major academia institutes that offer master programs in cyber security. Furthermore, the chapter attempts to bridge the gap between the different audiences. The gap is so broad that the term cyber security is not agreed upon even in spelling. Then, the chapter presents the suggested body of knowledge.

The research first discusses the notation of body of knowledge: discussing the definition, incentive, and mechanism. The accreditation process is the application of the body of knowledge; hence accreditation and accreditation incentive are discussed and the ACM & IEEE development of body of knowledge to different disciplines in the Information Technology Arena.

The research then addresses duality of spelling of the term cyber security versus cybersecurity, both are used interchangeably. This discrepancy in spelling the term serves as the base gap among the cybersecurity community. While such a gap must be bridged commencing with reaching an agreement on one spelling, however, in the scope section, a framework of elements is suggested to at least limit the intrusions of some unrelated terms.

Then, the research gives a presentation about cyber security in the academic arena. The showcase of academic perspective of cyber security included 61 master programs and 17 different countries namely Australia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, India, Italy, Lithuania, Malaysia, Malta, Netherlands, New Zealand, Spain, UK, USA. The showcase presented the many irregularities and anomalies of cyber security master programs. Next, the chapter sheds the light on cyber security from Practitioner Perspective, citing the work NICE to standardize the body of knowledge of cyber security. The research concludes with a suggested body of knowledge for cyber security. Based on a comprehensive definition of cyber security, the chapter also suggested two matrices that represent the interaction among the different elements of computer system with physical and non-physical threats, and a matrix that shows the interaction of physical/ non-physical threats with conductor of the threat internal and external. Furthermore, the final section presents and explains the core elements of the cyber security. This research is an expansion from a paper titled Cyber Security discussed in SC2 IEEE conference [1].

2. Body of knowledge

This section covers four topics to be discussed: first, the definition of body of knowledge and what incites the development of body of knowledge, further, giving examples about the body of knowledge in the different disciplines. The next two sections discuss the accreditation bodies and the incentive of accreditations. The last section discusses ACM & IEEE efforts in developing body of knowledge to different disciplines in the Information Technology arena.

2.1. Body of knowledge: definitions, incentives, and examples

Body of knowledge (BOK) is best stated by [2] "(1) structured knowledge that is used by members of a discipline to guide their practice or work." (2) "The prescribed aggregation of knowledge in a particular area an individual is expected to have mastered to be considered or certified as a practitioner." Another definition of BOK is by [3] "A BOK is a term used to represent the complete set of concepts, terms, and activities that make up a professional Domain. It encompasses the core teachings, skills, and research in a field or industry."

There are many incentives to build a BOK in different disciplines cited by many researchers: [4] said that "BOK describes relevant knowledge for a discipline and will need show the consensus in the Knowledge Areas (KA), and related disciplines"; in addition, the same source states that BOK is useful for curricula design for innovation while industry context present. [5] said that BOK is a practice to support education, research, professional development, and practice. Furthermore, [6] listed that BOK will allow to meet the challenge of rapidly changing landscape and the challenge of accommodating the diversity of emerging technologies. Again, the same source recites that BOK is used in curricula development, and BOK is the basis of evaluating the knowledge and skills of the discipline graduates, hence providing a roadmap to follow.

In different disciplines, there are many BOK, for example: Systems engineering (G2SEBoK), Information systems engineering (ISEBOK), Software engineering (SWEBOK) [5–7], Information Technology (ITBOK), Project management (PMBOK-1, PMBOK-2), Body of Quality Knowledge (BOQK), New Product Development Body of Knowledge (NPDBOK), Software Requirements Traceability Body of Knowledge [8], Canadian IT Body of Knowledge, Civil Engineering Body of Knowledge, Geographic Information Science and Technology Body of Knowledge, Project Management Body of Knowledge, Business Analysis Body of Knowledge, The requirements engineering body of knowledge (rebok) [3].

2.2. Accreditation bodies

The ultimate goal of accreditation bodies of higher education is to first standardize education and maintain the quality of education in the different educational institutes. The second is to enhance the credit transferability among different educational institutes and furthermore different countries. Next, we present some international and national quality assurance and accreditation organizations from Germany, Spain, Hong Kong, Pakistan, Canada, Swiss, Austria, and USA. In addition, there are two important information technology-based organizations: ABET which is IEEE-based organization and ACM.

Internationally, there are two organizations: The International Network for Quality Assurance Agencies in Higher Education (INQAAHE) which has 280 members [9]. The second is US-based organization; Council for Higher Education Accreditation has 467 quality assurance bodies, accreditation bodies, and ministries of Education from 175 countries, and has 3000 member institutions [10]. CHEA is a member in INQAAHE. CHEA replaced Council on Postsecondary Accreditation (COPA) and Federation of Regional Accrediting Commissions of Higher Education (FRACHE). In Europe, there is European Association for Quality Assurance in Higher Education (ENQA) which has 51 organizations and 28 countries. ENQA [11] established The European Quality Assurance Register for Higher Education (EQAR), the European Students' Union (ESI), the European University Association (EUA), and the European Association of Institutions in Higher Education (EURASHE), and ENIC-NARIC (National Academic Recognition Information Centre) comprises all countries of Europe as well as Australia, Canada, Israel, the United States of America, and New Zealand.

In Germany, Kultusministerkonferenz (KMK) [12] was founded in 1948, and then in 1957, German *Council of Science and Humanities* (Wissenschaftsrat) was founded. KMK established *Accreditation Council* (Akkreditierungsrat). Associated with the Accreditation Council, 10 agencies are as follows: Swiss Agency for Accreditation and Quality Assurance(AAQ), Accreditation, Certification and Quality Assurance Institute (ACQUIN), Accreditation Agency for Study Programmes in Health and Social Sciences (AHPGS), Agency for Quality Assurance and Accreditation of Canonical Study Programmes (AKAST), Agency for Quality Assurance and Accreditation Austria(AQ Austria), Agency for Quality Assurance by Accreditation of Study Programmes (AQAS), Accreditation Agency for Degree Programmes in Engineering, Informatics/Computer Science, the Natural Sciences and Mathematics (ASIIN), evaluation agency Baden-Württemberg(evalag), Foundation for International Business Administration Accreditation (FIBAA), and Central Evaluation and Accreditation Agency Hannover (ZEvA).

In Spain, the *Agencia Nacional de la Evaluación de la Calidad y Acreditación* (National Agency for Quality Assessment and Accreditation), which is dubbed (ANECA), was founded in 2002 [13]. ANECA is a full member of European Association for Quality Assurance in Higher Education (ENQA), International Network for Quality Assurance Agencies in Higher Education (INQAAHE), and European Quality Assurance Register for Higher Education (EQAR).

In the United Kingdom, there is Quality Assurance Agency (QAA) which is a member of INQAAHE and ENQA [14]. In Hong Kong, the Hong Kong Council for Accreditation of Academic and Vocational Qualifications (HKCAAVQ) replaced the Hong Kong Council for Academic Accreditation [15].

In India, there are 12 professional councils: All India Council for Technical Education (AICTE), Distance Education Council (DEC), Indian Council for Agriculture Research (ICAR), Bar Council of India (BCI), National Council for Teacher Education (NCTE), Rehabilitation Council of India (RCI), Medical Council of India (MCI), Pharmacy Council of India (PCI), Indian Nursing Council (INC), Dentist Council of India (DCI), Central Council of Homeopathy (CCH), and Central Council of Indian Medicine (CCIM) [16].

In Pakistan, under Quality Assurance Agency of Higher Education Commission of Pakistan, there are National Accreditation Council for Teachers Education (NACTE), National Agricultural Education Accreditation Council (NAEAC), National Business Education Accreditation Council (NBEAC), and National Computing Education Accreditation Council (NCEAC) [17–20].

In Canada, the Canada's Association of I.T. Professional (CIPS) is a Full Member of the Association of Accrediting Agencies of Canada (AAAC). CIPS has established the Computer Science Accreditation Council (CSAC), the Information Systems and Technology Accreditation Council (ISTAC) and the Business Technology Management Accreditation Council (BTMAC) as autonomous bodies. CIPS was established with this name in 1968. CIPS accredits the University, college/applied degree programs. The programs include Computer Science Degree Programs, Software Engineering Degree Programs, Interdisciplinary Programs, Management Information Systems Degree Programs, Business Management Technology Programs, Computer Systems Technology type Diploma Programs, and Applied Information Technology Degree Programs.

http://dx.doi.org/10.5772/intechopen.77975

In the USA, the *Higher education accreditation in the United States* is categorized: regional, national, programmatic, and faith-based accreditors. There are six regional accreditors namely Middle States Commission on Higher Education, New England Association of Schools and Colleges, Northwest Commission on Colleges and Universities (NWCCU), Higher Learning Commission (HLC) (formerly, North Central Association of Colleges and Schools (NCA)), Southern Association of Colleges and Schools (SACS) Commission on Colleges, and Western Association of Schools and Colleges (WASC-ACCJC). There are six national accreditors (nationwide not international): Accrediting Bureau of Health Education Schools (ABHES) (recognized by USDE), Accrediting Commission of Career Schools and Colleges (ACCSC) (recognized by USDE), Accrediting Council for Continuing Education and Training (ACCET) (recognized by USDE), Council on Occupational Education (COE) (recognized by USDE), Distance Education Accrediting Commission (DEAC) (recognized by USDE and CHEA), and Accrediting Council for Independent Colleges and Schools (ACICS) [21]. The specialized or programmatic accreditors are generally under CHEA or Department of Education US (USDE), and there are 76 agencies.

ABET is programmatic Accreditation established in 1932 and has 3369 programs [10]. ABET accredited 3852 programs at 776 colleges and universities in 31 countries according to [22]. ABET covers disciplines of applied and natural science, computing, engineering, and engineering technology at the associate, bachelor, and master degree levels. ABET has four accreditation commissions: Applied and Natural Science Accreditation Commission (ANSAC), Computing Accreditation Commission (CAC), Engineering Accreditation Commission (EAC), and Engineering Technology Accreditation Commission (ETAC). ABET is a federation of 35 societies and organizations [22]; furthermore, ABET stemmed from seven engineering societies. The first computer engineering program accredited by ABET was in 1971 at Case Western Reserve University [25]. Another report was published for the body of knowledge for Information Technology; the report is 161 pages long.

The Association for Computing Machinery (ACM) established in 1947 has 100,000 members. ACM is an organization for academic and scholarly interest in computer science. ACM has 171 local chapters, 37 special interest groups, and more than 50 scholarly peer-reviewed journals [23].

2.3. Why accredit

A body of knowledge "can be very useful to provide a comprehensive and integrative view of the discipline, for assessment of professionals and organizations, for self-assessment as well as for curriculum development for academic or professional development courses and degree programs" [2]. Accreditation in accordance to body of knowledge affects students, institutions, public, and professionals. In fact, accreditation is the process and implementation phase of the body of knowledge. The ultimate goal of both the idea (body of knowledge) and the process (accreditation) is to create a better-educated computer professional. Such computer professional shall practice with an ethical manner to the well-being of the ordinary user, organization, establishment, and the public. Such professional is required in industry and government, and hence, all parties need to cooperate to create the proper environment for such professional to spring to life. Industry standards must be met by the Institutes in the supply–demand manners. Furthermore, properly accredited institute can provide computer

students with proper education that will prepare them to further advance their higher education. Also, institutes can self-evaluate, analyze, and bridge the gap between industry and education.

The accreditation process must be fair, unswerving, confidential with clear process, transparent, and objective. The accreditation agency must be independent and autonomous from educational institute. The accreditation process must be carried out by qualified reviewers. Resources must be available to carry process effectively. Accreditation process, goals, steps, and time must be clear and set, and such guidelines are set by [24].

2.4. ACM and IEEE efforts in body of knowledge

ACM and IEEE developed a body of knowledge, explained in a report published in 15/Dec/2016 as shown in [25]. The report was developed by two delegations, both represented ACM and IEEE computer society delegates came from USA, China, and Scotland from 10 universities and IBM. The delegates came from 10 universities namely Hofstra University (USA), Milwaukee School of Engineering (USA), Clarkson University (USA), University of Florida (USA), Georgia Institute of Technology (USA), Mississippi State University (USA), Tsinghua University (China), Peking University (China), University of Strathclyde (Scotland), and Auburn University (USA). The delegates were four from IEEE and seven from ACM.

The report describes in five specialties pertaining to computers and leaves the sixth for future model. The report lists 14 underlying principles that guide the committee through the description of the body of knowledge as seen in pages 14 and 15 of the report [25]. In Chapter 3 of the document, the body of knowledge of *Computing engineering* was described in detail. In 2013, a report was published for the computer science curricula [26], and the body of knowledge of *computer science* was discussed in Chapter 4 of the 518-page document.

In 2016, C.C. Walrad said "the IEEE Computer Society's (CS's) Educational Activities Board merged with the Professional Activities Board to form the Professional and Educational Activities Board (PEAB) in 2015. This merger facilitated the development of the Guide to the *Software Engineering Body of Knowledge* (SWEBOK) and training in the SWEBOK knowledge areas, as well as coordination of IT curriculum development activities and the creation of a Guide to the Enterprise IT Body of Knowledge (EITBOK), which will be available in wiki form later this year. Moreover, the merger serves to strengthen the CS's joint work with ACM" [27].

In 2017, a report was published for Information Technology curricula [28]. The body of knowledge was discussed in Chapter 6. Chapter 6 discussed four topics: structure of IT curricula framework, distilling the IT curricular framework, IT domain clusters, and contemporary illustration of IT.

3. Cyber security scope

The term cyber security has a duality: some write the term as one word, while others write the term as two words; accordingly, this is the key gap within all players in the cyber security community, which could be overcome by reaching a unanimous decision on one spelling. In

http://dx.doi.org/10.5772/intechopen.77975

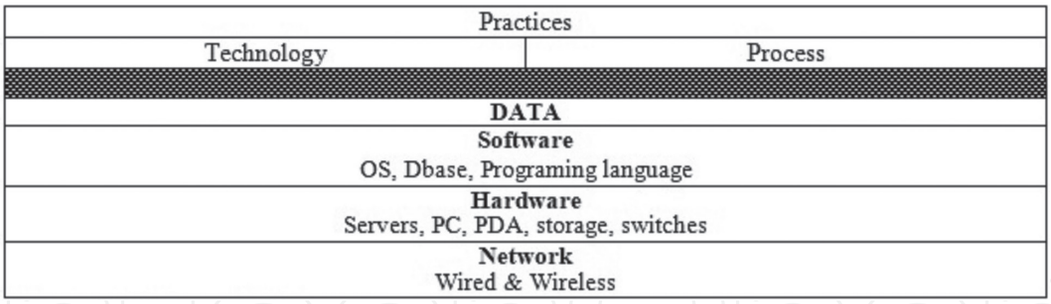

Figure 1. Cyber security elements.

the scope section, a framework of elements is suggested to at least limit the intrusions of some unrelated terms; as such, in this section, the chapter presents the different discussions about the definition of the term "cyber security." Moreover, the section illustrates the elements of the cyber security framework, as shown in **Figure 1**.

Most importantly is to define cyber security, which entails cyber security as "The ability to protect or defend the use of cyberspace from cyber-attacks" [29], using the term as one word. However, in 2014, [30] conducted a whole research to clarify the ambiguity of the term. In this context, the authors of the chapter found nine different definitions and came up with the 10th definition, denoted as "Craigen's definition" as follows: "Cyber security is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." Cyber security entails protecting *what from who* and *means* of protection; [31, 32].

The three parts of the definition drive each other; the *what* part of the definition includes hardware, software, network, and data, the *means* of protection are practices, technology, and process, while the *from who* part of the definitions includes internal and external/hostile or naïve threats and attacks. In this token, the different attacks rely on the technology and its development, and so the *means* of protection relies on the technology and how attacks are dealt with, thereby creating a vicious cycle.

4. Cyber security in academia

This section discusses the flounder of the academic arena regarding cyber security. The study reviewed a total of 61 master programs in 61 institute, 19 of them were studied with details of courses offered. Geographically, the study covered 17 different countries that are considered well developed, with respect to Information Technology namely Australia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, India, Italy, Lithuania, Malaysia, Malta, Netherlands, New Zealand, Spain, UK, and USA.

Table 1 illustrates the number of master programs distributed geographically, which highlights that UK and USA have the most master programs pertaining to cyber security, where USA has 25 master programs, followed by UK with 16 master programs, whereas Spain, Estonia, Finland, France, and Netherlands follow with two programs, and the remaining 10 countries with only one program each.

Country	Number of programs
Australia	1
Cyprus	1
Czech Republic	1
Estonia	2
Finland	2
France	2
Germany	1
India	1
Italy	1
Lithuania	1
Malaysia	1
Malta	1
Netherlands	2
New Zealand	1
Spain	2
UK	16
USA	25
Total	61

Table 1. Master programs in different countries.

In light of the abovementioned, it is worth noting that a report, by professor Andrew McGettrick, the Chair of Education Board in ACM, titled "Toward Curricular Guidelines for Cyber security" within "Report of a Workshop on Cyber security Education and Training "clearly stated that "Cyber security is currently an immature and ill-defined subject and not a true discipline since it lacks some of the criteria normally applied to disciplines" [33].

4.1. Cyber security trending in academia

Academia is supposed to lead the world in standardization and setting the rules. Yet, in this case, academia is at loss for the following reasons: first, there is a discrepancy in the wording of the term cyber security; some use "Cyber Security," others use "Cybersecurity," and others use the term "security." Second, the offering of cyber security master program is under the umbrella of Master of Science, Master of Arts, engineering, criminal justice. Third, the faculty conducting the program is computer science, engineering, business, management, Arts and Social Sciences. Fourth, the master program is offered online, traditional, and distance learning. Fifth, in research, the only paper tackled the subject was [34], which discussed the need from *JOB POSTING* perspective. In the next section, each of reasons will be presented along

with 61 different master programs offered worldwide with each program the university, faculty, and country, shown in Appendix A.

In respect to the term cyber security, being used as two separate words "Cyber Security," 17 universities used it, namely KL University, North Umbria University London Campus, The University of Waikato, University of Westminster, University of Greenwich, Tallinn University of Technology, The University of Warwick, Harbour Space, Saint Peter's University, Estonian Information Technology College, University of Southern California, The University of San Diego, Wright State University, University of York, University of south Australia, Temple University, George Mason University. On the other hand, 16 institutes used the term "Cybersecurity," as one word, namely The George Washington University, St. Mary's University, University of Central Missouri, Webster University Leiden, University of Maryland, University of Dallas College of Business, Sacred Heart University, Johns Hopkins, University of Maryland, NYU Tandon School of Engineering, University Of South Florida, Fordham University, University of Dallas, Villanova University, Embry-Riddle Aeronautical University, John Jay College of Criminal Justice. However, other terms referring to the term "Cybersecurity" like "Information Security" and "Digital Security" were used in the naming of the master program namely University of Turku, University of Kent, Eurecom, Asia Pacific University of Technology & Innovation (Apu), Cardiff University, Ferris State University, Vilnius Gediminas Technical University.

Moreover, the term "security" was used in nine program names to show that the program is related to the issue, namely: The University of Findlay, Eit Digital Master School, Cranfield University, Edinburgh Napier University, University of Amsterdam, Brunel University, Leeds Beckett University, Aalto University, and Esiea Graduate Engineering School.

The programs were offered as Master of Science (MSC) in the faculty of computer science like University of Maryland, University of York or engineering like Villanova University, University of Southern California; still, others offered their program as a Master of Arts (MA) or under the faculty of Business like Brunel University and Temple University or faculty of management like University of San Francisco or faculty of criminal justice like John Jay College of Criminal Justice.

On a different note, while Brunel University program is a distance learning type, some institutions offer "Cyber security" programs online such as University of Liverpool, University of The Cumberlands, Norwich University, NYU Tandon, whereas others require a traditional way of teaching.

According to numerous academic programs, "Cyber security" is referred to as digital security. In fact, there are 19 different names that pertain to cyber security according to different academic programs, inter alia: Digital Forensics, Network Security, Applied Security and Analytics, Security and Privacy, Information Security and Cryptography, Forensics, Electronic Warfare, Counter Terrorism and Organized Crime, Information Security and Biometrics, Security and Management, Information Technologies Security, Intelligence and Security Studies, Information Security & Privacy, Information Assurance, in Network Security and Pen Testing, Cyber Security Engineering, Network & Information Security, Operations and Leadership, IT Auditing and Cyber Security.

The chapter reviewed the 61 master programs listed in Appendix A, of which 19 disclosed their detailed classes offered within their respective programs. In turn, the researcher studied 110 different classes offered within the 19 programs and found the following: (1) six programs listed a course pertaining to programming and algorithms; (2) five programs listed a course pertaining to assurance using titles like Computer Systems Assurance Units, Development of high assurance systems, Information Assurance, Information Assurance and Security; (3) one master program offered a course about auditing entitled "*Software Security Assessment*"; (4) seven programs offered a course about cryptography under different titles like *Applied Cryptography*, *Mathematics for Cryptography*; (5) one program covered database courses; (6) seven programs offered Forensics under different titles like *Cyber-crime and Computer Forensics*, *Digital Forensics*, *e-Crime*, *e-Discovery and Forensic Readiness*, *Forensic Computing*, *Network* and *Internet Forensics*; (7) four programs offered Identity with titles like *Identity and Access Management*, and *Identity Management for Federal IT*; (8) four programs offered courses pertaining to Law and Ethics, such as *Information Security and Ethics*, *Cyber Security Operational Policy*, *Human Aspects of Cyber security*: *Law, Ethics and Privacy* as well as *Introduction to Ethical Hacking*; (9) 13 programs offered curses on Networks, ranking the topic as the highest to be offered under different titles: *Advanced Network and Data Communication*, *Computer networking*, *Cryptography & Network Security*, *Cyber Network Security*, *Network and Internet Forensics*, *Network Essentials Intensive*, *Network Security*, *Network Visualization and Vulnerability Detection*, *Networks and Protocols*, and *Security applications in networking and distributed systems*; (10) five programs covered the topic Operating systems (OS) under related titles: *Operating Systems Security*, *Practical Unix*, and *Secure Operating Systems*; (11) eight programs offered Windows Administration; (12) eight programs offered Software engineering under different titles: *Information System Infrastructure Lifecycle Management*, *Complex Systems Engineering Management*, *Secure Software Design and Development*, *Software Engineering & Design*, *Software engineering*, *Software Security Lifecycle*, *Trusted System Design*, *Analysis* and *Development Units*; (13) four programs covered Digital logic and microprocessors design under different descriptions: *Computer Architecture*, *Secure Systems Architecture*, *Securing Digital Infrastructure*, and *Computer systems*; (14) more significantly is that 14 master programs used the term security vaguely in a number of courses, utilizing it as follows: *Information Security*, *Application Security*, *Best* Practices Managing Security and Privacy for Cloud Computing, Computer Security and Privacy, Computer Security Fundamentals, *Computer Security*, *Critical Infrastructure and Control System Security*, *Cyber Network Security*, *Cyber security Essentials*, *Foundations of Cyber Security*, *Hardware Security*, *Host Computer Security*, *Information*, *Security and Privacy*, as well as *Management and Cyber Security*.

In all the 19 master programs, there are 18 courses that are of special interest to cyber security:

1. Intrusion Detection
2. Advanced Penetration Testing
3. Cyber Fraud and Theft
4. Cyber Incident Handling and Response

http://dx.doi.org/10.5772/intechopen.77975

5. Cyber Incident Response and Computer Network Forensics
6. Cyber Intelligence
7. Cyber Intelligence & Counterintelligence
8. Cyber Security: Emerging Threats and Countermeasures
9. Cyber Terrorism
10. Cyber Security: Threats and Defense
11. Electronic Evidence Analysis and Presentation
12. Imaging for Security Applications Watermarking & Biometrics
13. Incident Detections & Responses
14. Intrusion Analysis and Response
15. Malware and Intrusion Detection
16. Security Attacks and Defenses
17. Security Tools for Information Security
18. System Exploitation and Penetration Testing

5. Cyber security from practitioner perspective

In this section, the chapter discusses the body of knowledge represented from a practitioner approach. Accordingly, the chapter researched the perspective of National Initiative for Cyber Security Education (NICE) and National Initiative for Cyber Security Careers and Studies (NICCS).

Managed by the Cyber Security Education and Awareness Branch (CE&A) within the Department of Homeland Security's (DHS) Office of Cyber security and Communications (CS&C), NICCS is an online resource for cyber security training that connects government employees, students, educators, and industry with cyber security training providers throughout the nation to ensure that the government workforce has the appropriate training and education in the cyber security field. Likewise, NICE is an initiative led by National Institute of Standards and Technology in the USA department of Commerce with partnership between government and academia focusing on cyber security training and education and workforce development; the NICE Program Office operates under the Applied Cyber security Division, positioning the program to support the ability of USA to address current and future cyber security challenges through standards and best practices [35], with the strategic intent to entice a nationwide dialogue, thereby leading an action on how to address the critical shortage of a skilled cyber security workforce.

Moreover, the NICE Cyber security Workforce Framework (NIST Special Publication 800–181) serves as a fundamental reference resource to improve the communication needed to identify, recruit, and develop cyber security talent. To reverse engineer and attempt to define the core body of knowledge, NICE limited The Cyber Security Work Categories to the following seven categories of common cyber security functions:

1. Operate and maintain
2. Securely provision
3. Protect and defend
4. Oversee and govern
5. Analyze
6. Investigate
7. Collect and operate.

In addition, NICE had in mind the following audience for the framework: employer, employee, training, education, and technology providers. Within this context, NICCS developed 17 focus areas of education used as guidelines to education institutions [36]:

1. *Cyber Investigations*: focuses on analyses of computer incidents and intrusions to determine attacker/source, infiltration path, mechanism, system modifications and effects, damages, exfiltration path, data exfiltrated, and residual effects.
2. *Data Management Systems Security*: concentrates on secure configuration, operation, and maintenance of databases and database management systems housing sensitive data.
3. *Data Security Analysis*: the analysis of data (e.g., system logs, network traffic) aims to identify suspected malicious activities.
4. *Digital Forensics*: the analysis of computer systems (hosts, servers, network components) aims to determine the effects that malware has had on the system.
5. *Health-Care Security*: focuses on design, development, operation, and maintenance of computer systems used in health-care applications.
6. *Industrial Control Systems—SCADA Security*: concentrates on design, development, operation, and maintenance of industrial control systems used in real-time infrastructures.
7. *Network Security Administration*: focuses on secure configuration, operation, and operation of an enterprise computer network.
8. *Network Security Engineering:* concentrates on the design of secure network infrastructures and security analysis of network traffic.
9. *Secure Cloud Computing*: targets design, development, operation, and maintenance of secure cloud architectures.

10. *Secure Embedded Systems*: concentrates on design, development, utilization, and management of secured embedded systems technologies.
11. *Secure Mobile Technology*: focuses on design, development, utilization, and management of secure mobile technologies, devices, and services.
12. *Secure Software Development*: revolves around the development of secure software.
13. *Secure Telecommunications*: involves design, development, and secure use of secure telecommunications systems whether the system is digital and analog.
14. *Security Incident Analysis and Response*: examines system vulnerability analysis and developing the right future response.
15. *Security Policy Development and Compliance*: revolves around the IT policy of an organization and the monitoring and evaluation tools related to such policy.
16. *Systems Security Administration*: focuses on secure configuration, operation, and maintenance of a computer system (host or workstation).
17. *Systems Security Engineering*: involves using system development life cycle while embedding and taking into account security issue.

6. Suggested cyber security body of knowledge

Cyber security encompasses physical and non-physical security of data, software, and hardware, from harm by both authorized and non-authorized access, whether access is internal or external. Cyber security is conducted via technology through predetermined processes. Since technology is advancing expeditiously, it is not only challenging but it is also imperative to predetermine the process of security; as such, several best practices and lessons learned are traded among practitioners.

The physical security of data software and hardware from authorized and non-authorized access includes but not limited to, protecting the server room, its location, the switches, the cable, data and data storage devices from fire, and excessive heat intruders. As such, server rooms are typically equipped with fire distinguisher, air conditioned, insulated from fire, and its floor is raised to docket the cables. In addition, the switches are usually installed in hidden high places to limit the reachability, and cables are docketed in walls or under a raised floor. The location of the server room is another issue that is part of physical security. The major issues that pertain to this subject are summarized in the subsequent matrix.

For authorized personnel, another layer of protection to access the IT systems should be in place, varying from setting up password-protected access or magnetic card to retina scan to lock and key, as illustrated in **Figure 2**. However, oftentimes, physical security and non-physical security are not confined to external threats and attackers and could be considered internally, in which case, if the assessed damage is considered either intentional or non-intentional. For intentional damage, a rigorous policy should be established to ensure employee compliance and discipline like cameras and employee follow-up; yet, non-intentional damage is alleviated by proper training and teaching.

	Physical	Non-physical
Data	Keep copies in different locations	Ciphering, password
Software		
• Operating system	Copies	Password/biometrics
• Application	Copies	Password/biometrics
Hardware		
• Network	Not visible	Password/biometrics
• Server	Location/fire distinguisher/air condition	Password/biometrics
• Switch	Location	Password/biometrics
• Cable	Embed in walls	Away from power

Figure 2. Matrix of interaction computer system with physical and non-physical threats.

	Physical	Non-physical
Internal	Damage to hardware & software (intentional or non-intentional) set policy and provide proper training	Viruses: limit access to external systems +policy
External	Physical attacks	Hacking +viruses: Fire walls + antivirus

Figure 3. Matrix that shows the interaction of physical/non-physical threats with conductor of the threat internal and external.

The non-physical damage is not only more sensitive but it is immensely difficult to follow, in view that the more significant threat comes from unlawful use and access to the system. Viruses are a major threat in this case, hence, limiting the access to the system by using strict policy and good antivirus may halt the effect.

The external threat of damage like hacking and viruses poses as the most challenging, albeit, software tools like firewall and antivirus may protect the system, as illustrated in **Figure 3**; however, external physical threat, such as attacking and looting ATM machines or physical attacks on server room, switches, cables, and data, can be overcome by setting up tangible measures. These methods can include, but not limited to, setting up servers in protected rooms, ensuring that switches and cables are not visible to external entities, and storing data in secure locations with copy and the use of enormous storage.

6.1. Core element in cyber security

The core elements in cyber security are the following 12 elements; these are the pillars or the base to any cyber security program:

1. Cyber Security Assurance
2. Cyber Security Assessment

3. Ciphering
4. Algorithms
5. Networks
6. Digital Logic and Microprocessors Design
7. Operating Systems
8. Database
9. Cyber Law & Ethics
10. Viruses & Hacking
11. Software Tools & Techniques
12. Software Auditing & Software Engineering.

The following will further explain the 12 pillars (see **Figure 4**) and core elements in the cyber security body of knowledge.

6.1.1. Cyber security assurance

Cyber security assurance is best defined by Lipner [37] and he also explained how to achieve security assurance. To define assurance, Lipner stated that "assurance: making systems that can resist attack." And he added "Assurance is achieved by integrating security into the process of designing, building, and testing systems" [37]. In a research conducted by [38] to develop Software Assurance Curriculum for master level and again in [39] to develop for Software Assurance Curriculum for master's level, the authors proposed a comprehensive curriculum specialized for software assurance. Cyber security special must learn method like *Mission Risk Diagnostic (MRD) described by* [40] used to assess risk in systems across the life cycle and supply chain. In addition, specialist must learn SQUARE. Security Quality Requirements Engineering (SQUARE) is a nine-step process that helps organizations build security, including privacy, into the early stages of the production lifecycle [41–43].

6.1.2. Cyber security assessment

Cyber security assessment is a process to assess an organization's level of risk and preparedness. The process is repeatable and measurable. The process has two parts: Inherent Risk Profile & Cyber security Maturity [44]. The assessments are conducted in domains according to five levels of maturity according to FFIEC [44] suggested model. According to [45], an assessment framework was developed and was adopted by 30% of US organizations. The framework provides a risk-based approach for cyber security through five core functions: identify, protect, detect, and respond and recovery. Furthermore, the cyber security

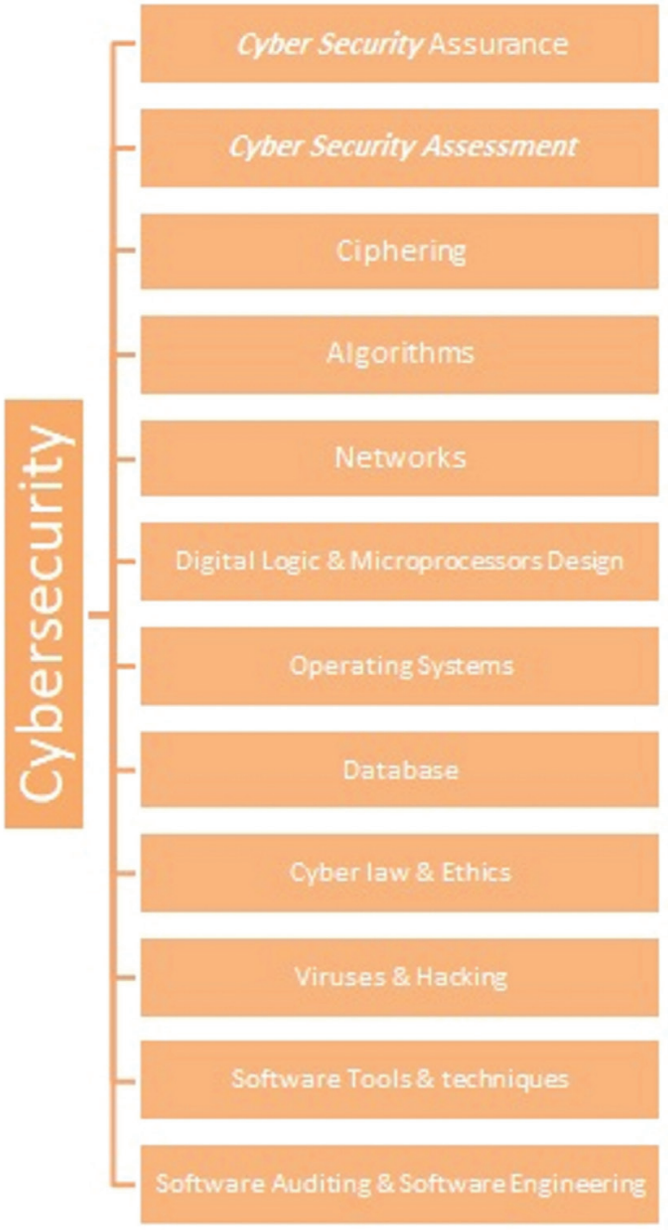

Figure 4. Pillars of cyber security.

professional should be able to create and conduct a cyber security assessment by understanding the various methodologies across all industries on how to conduct and manage a cyber security assessment, risk analysis, and how to mitigate various cyber security threats by conducting the following: first, understand and write reports on cyber threat attack analysis. Second, understand and write cyber security policy based on assessments. Third, detect and analyze incidents of action of attacks and threats. Fourth, establish cyber security controls based on established models and frameworks. Fifth, manage attack countermeasures. Sixth, mitigate risks of threats and attacks. Seventh, cycling of reports and evidence procedures for prosecution after such assessments have been produced.

http://dx.doi.org/10.5772/intechopen.77975

6.1.3. Ciphering

Ciphering is an essential part of security that allows the data to be transferred from point to point safely and without allowing anyone to look at the data being transferred. Ciphering is an old technique yet still needed for security. There are many types of ciphering that entails hardware and software, tools and techniques in addition to ciphering algorithms. Ciphering algorithms can be classified according to key as symmetrical and a symmetrical, according to type of operations conducted: substitution, transposition, bit manipulation, and to the cipher process block or stream cipher. Hence, public key ciphering RSA, and block cipher algorithms like IDEA, RC2, RC5, CAST, ElGamel, DSA, and Skipjack are important for the cyber security specialist. Topics like cryptanalysis, hash functions, digital signatures, and web security should be covered in detail.

6.1.4. Algorithms

Algorithms are the backbone of software. To develop any software, one must understand the logic behind the building blocks of the software. Algorithms deal with data taking into account speed, space storage, and time complexity. Search, sort, compression, and data structure are all based on algorithms. Algorithm is the language that a programmer, analyst, designer speaks with the computer to materialize their idea into working software. Hence, developing the logical sense to security specialist is a must trait. Typical course must include the following in the syllabus: sort & search algorithms, graph algorithms (Graph traversal (DFS, BFS) and applications, Connectivity, strong connectivity, bi-connectivity, Minimum spanning tree, Shortest path, Matchings, Network flow), and hard problems (Traveling salesman problem, Longest path, Hamilton cycle, Boolean circuit satisfiability, Clique, Vertex cover). Algorithm design: Divide-and-conquer, Graph traversal, Greedy, Dynamic Programming, Reductions, Use of advanced data structures. Algorithm correctness: Proofs and proof techniques (assumptions, basic logic inference and induction), Tree and graph properties. Algorithm analysis: Time and space complexity, Asymptotic analysis: Big Oh, Little oh, Theta, Worst case and average case analysis, Lower bounds. Tractable and intractable problems: Polynomial time algorithms, NP algorithms, NP hardness and NP completeness, NP Reductions.

6.1.5. Networks

Networks are a backbone of the data transfer; it is the roads to cars. The types and standards of networks are essential to anyone working in the cyber security. Networks are not only hardware they are standards, and routing algorithm, in addition to hubs, switches, cables, and jacks. Furthermore, the security models of computer networks along with ISO standard of these models, that is, Open Systems Interconnection (OSI), and transmission control protocol and Internet protocol (TCP/IP). Typically, a network course covers the following topics: Fundamentals, Link Layer, Media Access, Internetworking, Routing, Transport Layer, and Application Layer. The Fundamentals & Link Layer which includes Building a network, Layering and protocols—Internet Architecture, Network software, Performance; Link layer Services: Framing, Error Detection, Flow control. The Media Access & Internetworking which

includes Media access control—Ethernet (802.3), Wireless LANs 802.11, Bluetooth, Switching and Bridging, Basic Internetworking (IP, CIDR, ARP, DHCP, and ICMP). The routing topic which includes Routing (RIP, OSPF, metrics), Switch basics—Global Internet (Areas, BGP, IPv6), Multicast addresses, multicast routing (DVMRP, PIM). The Transport Layer topic which includes Overview of Transport layer, UDP, Reliable byte stream (TCP), Connection management, Flow control, Retransmission, TCP Congestion control, Congestion avoidance (DECbit, RED), QoS, Application requirements. The Application Layer which includes Traditional applications: Electronic Mail (SMTP, POP3, IMAP, MIME), HTTP, Web Services, DNS, and SNMP.

6.1.6. Digital logic and microprocessors design

Digital logic and microprocessors design are basic and fundamental for cyber security. Under this topic, things like the principles of programmable logic devices, combinational and sequential circuits, and the principles of hardware design, the structure and electronic design of modern processors. In addition, logical gates, flip-flop, and binary world are included.

6.1.7. Operating systems

Operating system (OS) is the layer of software that lay between hardware and applications. Through OS, a person can speak to the computer hardware using a programming language. The essentials under this topic are processes and threads, mutual exclusion, CPU scheduling, deadlock, memory management, and file systems, distributed systems.

6.1.8. Database

Database is where data are stored in a computer system, topics under database are (but not limited to) data models like Entity Relations (ER), relational; query languages including relational algebra, Structure Query Language (SQL); implementation techniques of database management systems including index structures, concurrency control, recovery, and query processing; management of semi-structured and complex data; distributed and NoSQL databases.

6.1.9. Cyber law and ethics

Knowing the difference between cyber laws and regulations to cyber security is like knowing the laws and regulations to policeman. It is essential to know cyber laws and regulation since borders do not exist in the cyber world. There also many ethical issues that pertain to the topic not to mention the power that comes with such territory.

6.1.10. Viruses, warms, and hacking

Cyber security specialist must be aware of the methods and tools and techniques used to counter affect viruses, warms, hacking the malware software in general. For a policeman to be good at his job, he must be aware of the criminal acts and how they are conducted.

Cyber security must know the different types of viruses, warms, and hacking methods in order to deal with such problems. Malware ranges from annoying malicious software to cyber-weapon that attacks and destroys. Furthermore, detection, analysis, control, and eradication of such software are essential part of cyber security education. Tools like Dependency Walker, Fakenet, FileAlyzer 2.0, HxD, IDA Free, ImpREC, LordPE, Malcode Analyst Pack, OllyDbg, PEiD, PEview, Regshot, Resource Hacker, Sysinternals Suite, UPX, Visual Studio, Windbg, Wireshark, System Monitor, Process Explorer, CaptureBAT, Regshot, VMware, BinText, LordPE, QuickUnpack, Firebug, PELister, PEiD, IDA Pro, OllyDbg and plug-ins such as OllyDump, HideOD, Rhino, Malzilla, SpiderMonkey, Jsunpack-n. Internet Explorer Developer Toolbar, cscript Honeyd, NetCat, Wireshark, curl, wget, xorsearch OfficeMalScanner, OffVis, Radare, FileInsight, malfind2, apihooks, SWFTools, Flare, and shellcode2exe are essential for cyber security expert.

6.1.11. Software tools and techniques

There are tremendous amount of software tools and techniques that is especially developed for cyber security. The simplest is antivirus software, database management software, operating systems management software, network management software, and so on. Hence, cyber security specialist must be familiar with these tools and techniques.

6.1.12. Software auditing and software engineering

Software auditing and software engineering is the 12th pillar that is of core importance to Cyber security. Most attacks on cyber systems are viruses or hacks coming from internal or external source, thereby misusing a vulnerability of software. For example, a programmer forgot to take into account certain case or a port. Software engineering should take the right measure so that such case does not occur. Regular auditing to software and data and building self-tests within the software will catch such problem beforehand. Hence, cyber security specialist must be aware of the tools, techniques, and methods of software engineering and auditing. Furthermore, security specialist must have the knowledge of Software Assurance Framework (SAF) explained in [46]. Software Assurance Framework (SAF) is a collection of cyber security practices that programs can apply across the acquisition lifecycle and supply chain. Hence, cyber security specialist must be aware of software security framework such as IMAF. IMAF is a framework suggested by [47] that aligns drivers with software security codes of practices. There are many codes of practices listed by [47]: Building Security in Maturity Model (BSIMM), Open Web Application Security Project (OWASP), Software Assurance Maturity Model (SAMM), Department of Homeland Security Measurement work and Assurance for CMMI Process Reference Model, and CERT Resilience Management Model.

None-core competencies and elements are important but since technology keeps changing, further courses can be developed through course training or self-training or both. Such elements include but not limited to Intrusion Detection (Analysis and Response), penetration testing, Intelligence & counterintelligence, and Electronic Evidence Analysis.

7. Conclusion

This research first discussed the body of knowledge notion and scope of cyber security definition and then gave a presentation about cyber security in the academic arena. The showcase of academic perspective of cyber security included the 61 master programs from 17 different countries namely Australia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, India, Italy, Lithuania, Malaysia, Malta, Netherlands, New Zealand, Spain, UK, and USA. The showcase presented the many irregularities and anomalies of cyber security master programs. Next, the chapter presented cyber security from practitioner perspective citing the work NICE to standardize the body of knowledge of cyber security from practitioner perspective. The last part of the chapter presents a suggested body of knowledge for cyber security. Based on a comprehensive definition of cyber security, the chapter also suggested two matrices that represent the interaction among the different elements of computer system with physical and non-physical threats, and a matrix that shows the interaction of physical/non-physical threats with conductor of the threat internal and external. Furthermore, the section presents and explains the core elements of the cyber security.

A. Master programs, their affiliation, country, and faculty

Name	Institute	Country	Faculty
MSc in Computer Science	University of Nicosia	Cyp	
MSc in cyber security in CS	The George Washington University	USA	Engineering & Applied Science
Master in Digital Security	Eurecom	Fr	
Master of Engineering in Cybersecurity	University of Maryland	USA	School of Engineering
MSc in Computer, Communication and Information Sciences - Security and Mobile Computing	Aalto University	Fin	
Mastère Spécialisé SIS: Sécurité de l'Information et des Systèmes	Esiea Graduate Engineering School	F	
Master of Information Systems	University Of San Francisco	USA	School of Management
Masters of Science in Engineering in Artificial Intelligence and Robotics	Sapienza University of Rome	It	
Digital Forensics and Cybersecurity programs	John Jay College of Criminal Justice	USA	
Master of Technology in Cyber Security and Digital Forensics	K L University	Ind	
Network Security and Pen Testing MSc	Middlesex University London	UK	
MSc Cyber Security	Northumbria University London Campus	UK	

http://dx.doi.org/10.5772/intechopen.77975

Name	Institute	Country	Faculty
Master of Cyber Security	The University of Waikato	New Z.	
MSc in Applied Security and Analytics	The University of Findlay	USA	
Master in Security and Privacy (S&P)	Eit Digital Master School	Ger	
Master's Degree Programme in Information Security and Cryptography	University of Turku	Fin	
Computer Engineering	International University Alliance	USA	
MSc Cyber Security and Forensics	University of Westminster	UK	Science and Technology
Electronic Warfare, Information and Cyber Degrees	Cranfield University	UK	
International Security Degrees	Cranfield University	UK	
Resilience, Counter Terrorism and Organized Crime Degrees	Cranfield University	UK	
MSc Computer Forensics & Cyber Security	University of Greenwich	UK	
MSc Advanced Security and Digital Forensics	Edinburgh Napier University	UK	
MSc in Cyber Security	Tallinn University of Technology	Estonia	
MSc Information Security and Biometrics	University of Kent	UK	
Master in Cyber Security and Management (CSM)	The University of Warwick	UK	Warwick Manufacturing Group Wmg
Master in Information Security	Harbour.Space	Spain	
Master of Information and Information Technologies Security	Vilnius Gediminas Technical University	LT	
1. MSc System and Network Engineering: Security	University of Amsterdam	NL	
MSc in Digital Security and Forensics	Asia Pacific University of Technology & Innovation (APU)	Mal	
MA Intelligence and Security Studies (Distance Learning)	Brunel University	UK	College of Business, Arts and Social Sciences
Master in Cybersecurity	St. Mary's University	USA	
Master in Cybersecurity	University of Central Missouri	USA	
MS Cybersecurity	Webster University Leiden	NL	
MSc Cyber Security Engineering (CSE)	The University of Warwick	UK	Warwick Manufacturing Group Wmg
MSc in Information Security & Privacy	Cardiff University	UK	
Master in Embedded Systems	Masaryk University	Czech R.	
MSc Digital Forensics and Security	Leeds Beckett University	U K	

Name	Institute	Country	Faculty
Master of Science in Cyber Security	Saint Peter's University	USA	
MSc in Cybersecurity (Information Assurance)	University of Dallas	USA	College of Business
MSc in Network Security and Pen Testing	Middlesex University Malta	Malta	
MSc in Information Security and Intelligence	Ferris State University	USA	
Masters in Cyber Security Engineering		Estonia	Information Technology College
MSc Network & Information Security	Kingston University London	UK	
Máster en Ciberseguridad UCAV-DELOITTE *	Universidad Católica De Ávila	Spain	
Master of Science: Cybersecurity	Sacred Heart University	USA	
MSc in Cybersecurity	Johns Hopkins	USA	Johns Hopkins Engineering
Master of Engineering in Cybersecurity	University of Maryland	USA	Computer Science
Master of Science Cyber Security Engineering	University of Southern California	USA	Viterbi School of Engineering
Cybersecurity Online	NYU Tandon School of Engineering	USA	
Cybersecurity Master's Degree	University of South Florida	USA	
MSc in Cybersecurity	Fordham University	USA	
Master of Science in Cyber Security Operations and Leadership	The University of San Diego	USA	
MSc in Cybersecurity	University of Dallas	USA	College of Business
MSc in Cyber Security	Wright State University	USA	The College of Engr & C S
MSc in Cybersecurity	Villanova University	USA	College of Engineering
MSc in Cyber Security	University of York	UK	Department of Comp. Sci.
MSc (Cyber Security and Forensic Computing)	University of South Australia	Aus	
IT Auditing and Cyber Security	Temple University	USA	Fox School of Business
Applied Information Technology, Cyber Security Concentration (MS)	George Mason University	USA	School of Engineering
MSc in Cybersecurity Engineering	Embry-Riddle Aeronautical University	USA	College of Engineering

Author details

Evon M Abu-Taieh[1]*, Auhood Abd. Al Faries[2,3], Shaha T. Alotaibi[2] and Ghadah Aldehim[2]

*Address all correspondence to: abutaieh@gmail.com

1 The University of Jordan, Aqaba, Jordan

2 Princess Nourah Bin Abdulrahman University, Saudi Arabia

3 King Saud University, Saudi Arabia

References

[1] Abu-Taieh E. Cyber Security Body of Knowledge. In: SC2 IEEE Conference; Japan. 2017

[2] Oren TI. Toward the body of knowledge of modeling and simulation. In: Interservice/ Industry Training, Simulation, and Education Conference (I/ITSEC) 2005; Orlando, FL. 2005

[3] Penzenstadler B, Fernandez M, Richardson D, Callele D, Wnuk K. The requirements engineering body of knowledge (rebok). In: 2013 21st IEEE International Requirements Engineering Conference (RE); Rio de Janeiro, Brasil. 2013

[4] Quezada-Sarmiento PA, Enciso-Quispe LE, Garbajosa J, Washizaki H. Curricular design based in bodies of knowledge: Engineering education for the innovation and the industry. In: SAI Computing Conference (SAI), 2016; London. 2016

[5] Adcock R, Hutchison N, Nielsen C. Defining an architecture for the systems engineering body of knowledge. In: 2016 Annual IEEE Systems Conference (SysCon); Orlando, FL. 2016

[6] Kajko-Mattsson M, Sjögren A, Lindbäck L. Everything is possible to structure—Even the software engineering body of knowledge. In: 2017 IEEE/ACM 1st International Workshop on Software Engineering Curricula for Millennials (SECM); Buenos Aires. 2017

[7] Bourque P, Fairley R. Guide to the Software Engineering Body of Knowledge (Swebok(R)): Version 3.0, 3ed ed. Los Alamitos, CA: IEEE Computer Society Press; 2014

[8] Duarte A, Duarte D, Thiry M. aceBoK: Toward a software requirements traceability body of knowledge. In: 2016 IEEE 24th International Requirements Engineering Conference (RE); Beijing. 2016

[9] INQAAHE. INQAAHE. 12 6 2017. [Online]. Available: http://www.inqaahe.org/presentation

[10] chea. 9 6 2017. [Online]. Available: http://www.chea.org/

[11] ENQA. 6 12 2017. [Online]. Available: Enqa.eu

[12] KMK. KMK. 12 6 2017. [Online]. Available: http://www.akkreditierungsrat.de/

[13] ANECA. 12 12 2017. [Online]. Available: www.aneca.es/

[14] PSRB. 5 5 2016. [Online]. Available: www.hesa.ac.uk

[15] hkcaavq. 12 12 2017. [Online]. Available: https://www.hkcaavq.edu.hk/en/

[16] HE_India. HE_India. Ministry of Human Resource Development Department of Higher Education. 12 12 2017. [Online]. Available: www.education.nic.in/higedu.asp

[17] NACTE. 12 12 2017. [Online]. Available: http://www.nacte.org.pk

[18] NAEAC. 12 12 2017. [Online]. Available: http://www.naeac.org.pk/

[19] NBEAC. 12 12 2017. [Online]. Available: www.pbeac.org.pk/

[20] NCEAC. 12 12 2017. [Online]. Available: http://www.nceac.org

[21] U.S. Department of Education. 9 8 2017. [Online]. Available: https://www2.ed.gov/admins/finaid/accred/accreditation_pg6.html

[22] ABET. ABET. 11 5 2017. [Online]. Available: http://www.abet.org/about-abet/

[23] ACM. About. 5 9 2017. [Online]. Available: www.acm.org

[24] CIPS. Accredited Programs. 11 5 2017. [Online]. Available: http://www.cips.ca/

[25] ACM, IEEE. Curriculum Guidelines for Undergraduate Degree Programs in Computer Engineering. New York: ACM IEEE; 2016

[26] ACM & IEEE. Curriculum Guidelines for Undergraduate Degree Programs in Computer Science. New York: ACM IEEE; 2013

[27] Walrad CC. The IEEE computer society and ACM's collaboration on computing education. Computer. 2016;**49**(3):88-91

[28] ACM & IEEE. Information Technology Curricula 2017. New York: Association for Computing Machinery (ACM) IEEE Computer Society (IEEE-CS); 2017

[29] Kissel R. Glossary of Key Information Security Terms. 5 2013. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf. [Accessed: 12.12.2017]

[30] Craigen D, Diakun-Thibault N, Purse R. Defining cybersecurity. Technology Innovation Management Review. 2014;**4**(10):13-21

[31] Davis Z. Definition of computer security. PCMag. 2017

[32] Gasser M. Building a Secure Computer System. 1st ed. USA: Van Nostrand Reinhold; 1988. p. 236. ISBN 0-442-23022-2

[33] McGettrick A. Toward Curricular Guidelines for Cybersecurity—Report of a Workshop on Cybersecurity Education and Training. ACM; 2013

[34] Benslimane Y, Yang Z, Bahli B. Information security between standards, certifications and technologies: An empirical study. In: 2016 International Conference on Information Science and Security (ICISS); Pattaya, Thailand. 2016

[35] NICE. National Initiative for Cybersecurity Education (NICE). 2 2013. [Online]. Available: https://www.nist.gov/itl/applied-Cybersecurity/nice/resources/nice-Cybersecurity-workforce-framework

[36] NICCS. 12 12 2017. [Online]. Available: https://niccs.us-cert.gov/sites/default/files/documents/pdf/cae_ia-cd_focusareas.pdf?trackDocs=cae_ia-cd_focusareas.pdf

[37] Lipner S. Security assurance. Communications of the ACM. 2015;**58**(11):24-26

[38] Mead N, Hilburn T, Linger R. Software Assurance Curriculum Project Volume II: Undergraduate Course Outlines(CMU/SEI-2010-TR-019). Pittsburgh, PA: Software Engineering Institute; 2010

[39] Mead N, Allen J, Ardis M, Hilburn T, Kornecki A, Linger R, McDonald J. Software Assurance Curriculum Project Volume I: Master of Software Assurance Reference Curriculum (CMU/SEI-2010-TR-005). Carnegie Mellon University; 2010

[40] Alberts C, Dorofee A. Mission Risk Diagnostic (MRD) Method Description (CMU/SEI-2012-TN-005). Pittsburgh, PA: Software Engineering Institute; 2012

[41] Chen P, Dean M, Ojoko-Adams D, Osman H, Lopez L, Xie N. Systems Quality Requirements Engineering (SQUARE) Methodology: Case Study on Asset Management System (CMU/SEI-2004-SR-015). Pittsburgh, PA: Software Engineering Institute; 2004

[42] Mouratidis H, Giorgini P. Integrating Security and Software Engineering: Advances and Future Visions. Hershey, PA: Idea Group Publishing; 2007

[43] Bijwe A, Mead N. Adapting the SQUARE Process for Privacy Requirements Engineering (CMU/SEI-2010-TN-022). Pittsburgh, PA: Software Engineering Institute; 2010

[44] FFIEC Cybersecurity Assessment Tool. USA: Federal Financial Institutions Examination Council; 2015

[45] Chabrow E. IST Unveils a Cybersecurity Self-Assessment Tool: Gauging the Effectiveness of Risk Management Initiatives. Princeton, NJ: Information Security Media Group Corp.; 2016

[46] Alberts C, Woody C. Prototype Software Assurance Framework (SAF):Introduction and Overview (CMU/SEI-2017-TN-001). Pittsburgh, PA: Software Engineering Institute; 2017

[47] Alberts C, Allen J, Stoddard R. Integrated Measurement and Analysis Framework for Software Security(CMU/SEI-2010-TN-025). Pittsburgh, PA: Software Engineering Institute; 2010

IntechOpen