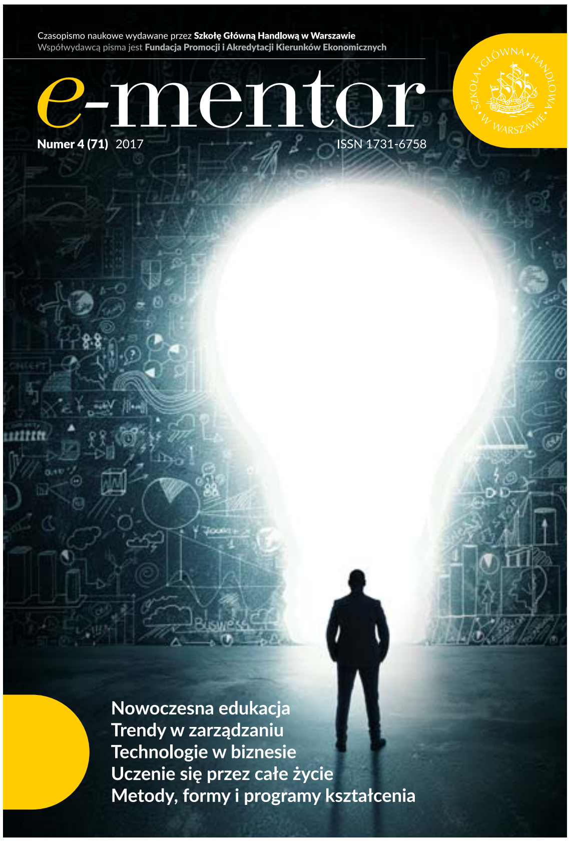
e-mentor

DWUMIESIĘCZNIK SZKOŁY GŁÓWNEJ HANDLOWEJ W WARSZAWIE
WSPÓŁWYDAWCA: FUNDACJA PROMOCJI I AKREDYTACJ KIERUNKÓW EKONOMICZNYCH


Czasopismo naukowe wydawane przez Szkołę Główną Handlową w Warszawie
Współwydawcą pisma jest Fundacja Promocji i Akredytacji Kierunków Ekonomicznych
e-mentor
Numer 4 (71) 2017
ISSN 1731-6758
SZKOŁA GŁÓWNA HANDLOWA W WARSZAWIE
Nowoczesna edukacja
Trendy w zarządzaniu
Technologie w biznesie
Uczenie się przez całe życie
Metody, formy i programy kształcenia

2017, nr 4 (71)

Andrzej J. Gapinski, *Certificate Programs in Computer Networks, Security, and Cloud Computing in the USA – A Review*, **„e-mentor" 2017, nr 4(71), s. 64–78, http://dx.doi.org/10.15219/em71.1313.**

Certificate Programs in Computer Networks, Security, and Cloud Computing in the USA – A Review

Andrzej J. Gapinski

The computer networks and security topics have been covered traditionally by computer science and information sciences and technology academic programs at numerous universities and colleges around the country. These themes have been the subject of specific courses within the respective undergraduate academic majors, graduate programs and certification programs. With the rapid advancement in computer technologies and their applications, the business world created the demand for specialists with appropriate knowledge and skills set associated with computer networks, cybersecurity, and recently added cloud computing services. To satisfy the job requirements often in niche areas, many certification programs were created by industry and academia, which complemented the 2-year or 4-year academic programs. The certification programs either augment skills set developed by academic degree programs or provide skilled workforce upon completion of relatively short in duration education or training programs through certification processes without completing lengthy academic degree curricula.

Scope of Certifications under Consideration

The article covers certificates in the area of computer networks, cybersecurity, and recently added cloud computing field that are offered by numerous academic institutions, various professional organizations, and other type of entities either private or public with focus on the USA. The review also provides a few examples of worldwide offerings with European – United Kingdom, Belgium, and Asian – Singapore certifications.

New Cybersecurity Threats

The new types of information security threats appeared relatively recently due to a combination of factors such as a wider adoption of cloud computing services by an increasing number of organizations around the world, and an increased number of attacks by malware in the form of ransomware, or insider threats, to name a few (Claycomb, 2012). These types of threats will only increase demand for skilled professionals and assign even more significance to information security implemented strategies and methods (Gapinski, 2014), training and certification.

New Threats Due to an Increased Role Played by Cloud Computing

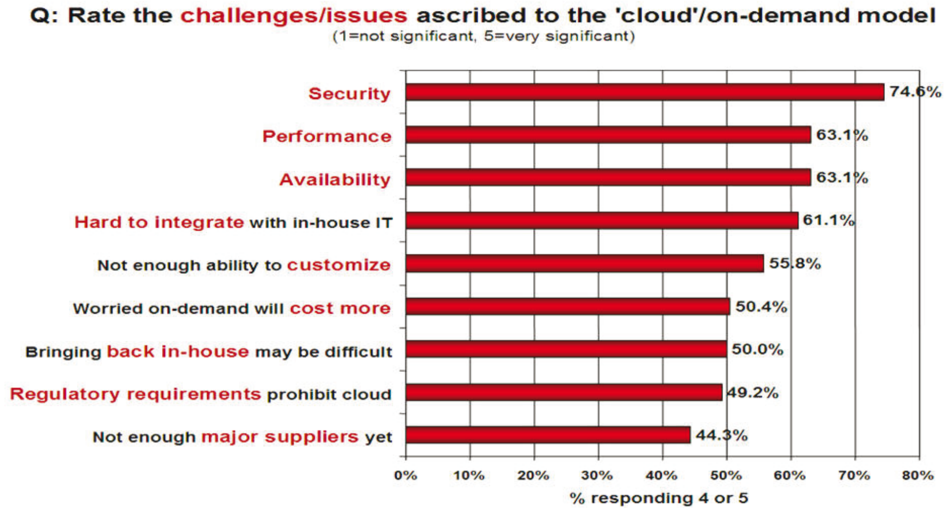
Cloud computing with its services as it increased its role and importance in data storage and processing for businesses worldwide created new challenges to information security with new concerns regarding confidentiality, integrity, and availability (Grobauer et al., 2011; Harfoushi et al., 2014; Pak, 2017). Cloud security problems may come from perceived or real loss of control, lack of trust, and/or multi-tenancy (Pak, 2017). Some of the threats may be caused by lack of understanding of the intricacies of sometime complex security policies offered by cloud computing vendors, by business and IT managers of companies using these services. The 2008 survey of business leaders performed by International Data Corporation (IDC), a UK firm, indicated significant concerns with cloud services as related to: security – 74.6 percent, performance – 63.1 percent, availability – 63.1 percent, integration with in-house IT processes – 61.1 percent, and ability to customize – 55.8 percent, among other factors (see Figure 1). Grobauer et al. (2011) analyzed cloud computing vulnerabilities and provided classification of threats based on type of cloud services (SaaS, PaaS, IaaS). Ristenpart et al. (2009) investigated cloud computing vulnerability due to possible "cross-VM information leakage." Gapinski (2014, 2015, 2016a) provided an overview of present day state and trends in cloud computing services including security concerns.

As cloud computing gains more popularity, the security concerns will only increase in importance.

Wireless Communication – Wi-Fi

Wireless communication introduced new vulnerabilities to network security due its novelty in wireless standards and established protocols. There are attempts to improve security of such networks (e.g. work by Balakrishnan, 2010). An increased popularity of Wi-Fi networks to provide communication services to customers worldwide, which offers often cost effectiveness over legacy solutions, combined with

Figure 1. Cloud computing challenges in the eyes of business leaders



Source: IDC Enterprise Panel, August 2008.

Wi-Fi protocols' vulnerabilities introduced new pathways for cybercrimes.

Ransomware

Ransomware according to Merriam-Webster (https://www.merriam-webster.com/dictionary/ransomware) is "a malware that requires the victim to pay a ransom to access encrypted files." As FORTINET (www.fortinet.com) in February, 2017, reported "a ransomware infects from 30,000 to 50,000 devices monthly, causing in 2016 year $850 million pay out by companies worldwide, while only 1 in 4 attacks is reported." Gravity of ransomware should not be underplayed considering that while ransomware provides only two percent of total malware attacks, it causes substantial damages to affected organizations "reaching $8,500 an hour of downtime," with organizations which do pay a ransom, "one in four never recovers the data" (http://www.fortinet.com). In addition, as FORTINET reports, "the ransomware is not blocked by traditional security methods," which only increases the severity of this threat.

Insider Threats

The security threats posed by insiders cannot be underestimated. These may include, according to Carnegie Mellon University, CERT (Claycomb, 2012): unauthorized access, unintentional exposure of sensitive data, malware code (viruses, warms, etc.), theft of intellectual property, or even intentional sabotage. Furthermore, CERT (Claycomb, 2012), reported that surveyed 607 organizations, of which 38 percent had more than 50,000 employees and 37 percent had less than 500 employees, 39 to 55 percent of them reported the significant insider security incidents (not just possible threats). CERT report (Claycomb, 2012) states that the vast majority "76% of such insider incidents are handled internally without any legal action or law enforcement and only 11% are handled externally with either law enforcement involvement or civil action." In addition, a significant number of individuals committing insider cybercrimes (e-crimes) could not be identified by internal investigations. Concerns about negative potential publicity played probably also a role why many insider cybercrime perpetrators were not prosecuted by companies. To address the issue effectively, the organizations may be in a position to introduce new behavioral-psychological measures and possibly inconspicuous screening of their employees with the help of artificial intelligence's methods and tools. The boundary between personal freedom and employers' rights may become even more skewed to the advantage of the business as businesses pursue their own market destiny and even economic survival. This is due to the fact that in the eyes of law the employee's privacy rights are subordinated to business rights (Stolfo et al., 2008). However, as Stolfo et al. (2008) pointed out, the psychological screening may bring false identification and negative consequence of "not hiring potential good employee" or hiring future cybercrime insider.

Cybersecurity Defined

A term cybersecurity or cyber security gets various interpretation, in either broader or narrower sense, depending on the circumstance and context. While cybersecurity in a broader interpretation is synonymous to IT security or information security, in a narrower sense it usually designates only security practices related to offensive and defensive actions in information systems (The Convergence of Operational Risk and Cyber Security, 2016).

The U.S. Department of Homeland Security (DoHS) describes the term as follows:

"A comprehensive cybersecurity program leverages industry standards and best practices to protect systems and detect potential problems, along with processes to be informed of current threats and enable timely response and recovery." (Homeland Security, 2017)

Techopedia (www.techopedia.com) offers the following description of cybersecurity:

"Cybersecurity refers to preventive methods to protect information from being stolen, compromised or attacked in some other way. It requires an understanding of potential information threats, such as viruses and other malicious code. Cybersecurity strategies include identity management, risk management, and incident management." (https://www.techopedia.com/definition/24747/cybersecurity)

Here, the description provided by Techopedia (https://www.techopedia.com/definition/24747/cybersecurity) of cybersecurity will be used.

Certificates and STEM Workforce

Certificate programs play an important role in preparing a workforce for current job openings through enhancing the knowledge of the professional workforce with the state of the art information on current technologies. Occupations in the area of computer networks and security belong to a general category of science, technology, engineering, and mathematics (STEM) professions. It is worthwhile to consider the significance of these professions in the context of the U.S. job market. According to the U.S. Department of Labor, Bureau of Labor Statistics (BLS) (www.bls.gov) data, the area of computer networks and security as a part of STEM disciplines shows an increase in employment on average of ten percent nationwide between 2009–2016 years (https://www.bls.gov; Gapinski, 2017). Within STEM occupations employment in computer related areas such as software developers, computer system analysts, computer support specialists, network and computer systems administrators and managers account for over two million job nationwide (Table 1; https://www.bls.gov).

Table 1. Employment for the largest STEM occupations, May 2015

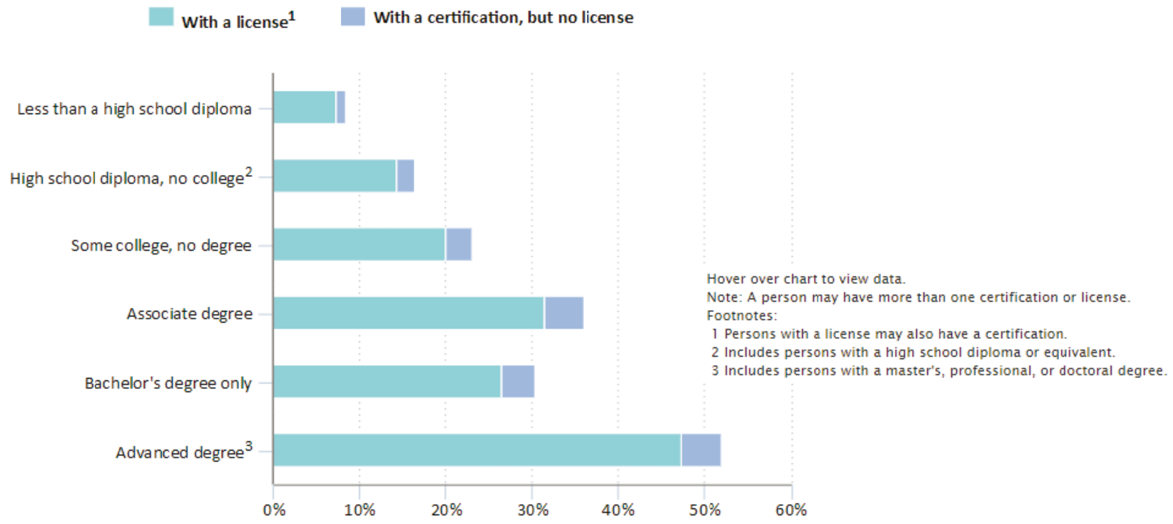
Largest USA STEM Occupations	Employment (jobs)
Software developers, applications	747,730
Computer user support specialists	585,060
Computer systems analysts	556,660
Software developers, systems software	390,750
Network and computer systems administrators	374,480
Computer and information systems managers	341,250
Sales representatives, wholesale and manufacturing, technical and scientific products	334,010
Computer programmers	289,420
Mechanical engineers	278,340
Civil engineers	275,210

Source: U.S. Dept. of Labor. Bureau of Labor Statistics (https://www.bls.gov).

CompTIA (https://certification.comptia.org), one of the IT certification organizations, claims that currently "IT positions make up 11% of all job openings."

How prevalent is the licensing and certification in the U.S. workforce as a measure of expected knowledge and skills set levels? According to the U.S. Bureau of Labor Statistics (BLS) (www.bls.gov) in 2015 about 22 percent of employed people had a license and 3 percent held a certification in various occupations. BLS reports (see Figure 2) that in 2015 out of 36 percent of the workforce with associate degrees, 31.4 percent held licensing and 4.6 percent a certificate. BLS states that 30.3 percent of workforce with a bachelor degree carried licensing – 26.4 percent and certificates

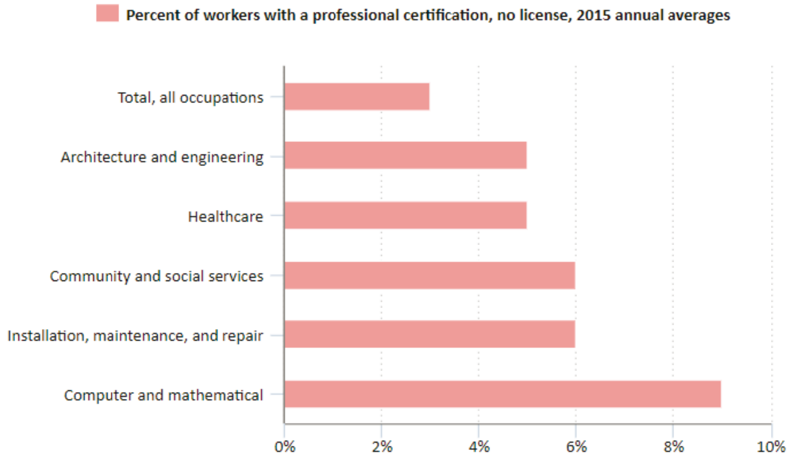
Figure 2. U.S. workforce – Employed 25 years or older with a license or certification by educational level (percent). 2015



Hover over chart to view data.
Note: A person may have more than one certification or license.
Footnotes:
1 Persons with a license may also have a certification.
2 Includes persons with a high school diploma or equivalent.
3 Includes persons with a master's, professional, or doctoral degree.

Source: U.S. Bureau of Labor Statistics.

Figure 3. U.S. workforce – Occupations with the highest percentages of workers with a professional certification (percent). 2015



Source: U.S. Bureau of Labor Statistics.

– 3.9 percent, and 52 percent of the workforce with an advanced education, which includes master, professional, and doctoral degrees carried a license – 47.3 percent and a certification – 4.7 percent (see Figure 2). With regard to STEM occupations related to the theme of the article, BLS reports that in 2015, nearly 9 percent of the 4.4 million workers in computer and math occupations had a certification but no license (see Figure 3).

The relative high percentages listed above are justified considering the fact that while universities and colleges do provide an educational foundation of knowledge and skills set for their graduates, the industry and service sectors do require specialized knowledge and skills set in very narrow fields of expertise. The industry and service sectors often provide incentives or funding to their employees to pursue certifications if it is not an entry requirement.

Consequently, considering the importance of information technology including computer networks and security in the national economy it is difficult not to emphasize the significance of the certification programs in the areas of high demand. Certifications play a vital role for professionals in staying current with rapidly changing technologies.

Assessing the Quality of a Certificate – Credentialing

Currently there is a rather large number of various certification programs offered worldwide including the USA by many vendors, professional organizations, and institutions of higher education, both public and private. The question arises: who checks and attests the quality of the certifications' offerings? The process of assessing and establishing the qualifications of licensed professionals and organizational entities is called credentialing.

The credentials usually are established through professional associations that organizations offering certification are members of. Namely, in many cases IT industry associations such as Computing Technology Industry Association (CompTIA, https://certification.comptia.org) are involved. In many instances the governmental agencies are involved by providing recognition and /or endorsement of the certifications. In the USA, it could be the Committee on National Security Systems (CNSS), a federal government entity under the U.S. Department of Defense to protect national security systems or the American National Standards Institute (ANSI).

Certifications: Where to Obtain Them?

The individuals seeking certification including the area of computer networks and security may seek certifications in a few ways. There are mainly four possible paths to get a certification (Wikipedia) from either: 1. Schools and universities; or 2. Corporation ("vendor") sponsored credentials (e.g., Microsoft, Cisco, etc.); or 3. Association and organization sponsored credentials; or 4. Governmental or quasi-government agencies. The last category may include, for example in the USA: U.S. Dept. of Defense (DoD), National Security Agency (NSA); and outside of the USA, EITCI (http://eitci.org) in Europe, and NICF in Singapore where National Infocomm Competency Framework (NICF, https://www.imda.gov.sg/industry-development/programmes-and-grants/individuals/national-infocomm-competency-framework-nicf), a quasi-governmental entity, sponsors training, licensure, certifications and credentialing via business partners.

Organizations Offering Information and Computer Security Certifications

There are many organizations in the USA and abroad that provide certification and education/training in computer networks and security. Many are non-profit entities set-up by various industry associations and some are offered by private for profit organizations in this field.

It is worthwhile to list the most valuable IT certifications at professional level based on salary data analysis (White and Hein, 2017; Half, 2017) that cover the information technology in a broad sense prior to reviewing certifications of a narrower topical scope of this paper (in alphabetical order):

- Amazon (http://www.amazon.com):
  - o AWS Certified Solutions Architect – Professional;
- ISACA (https://www.isaca.org) (IT audit control, security management, risk management, assessment, and mitigation, governance and compliance):
  - o Certified in the Governance of Enterprise IT (CGEIT),
  - o Certified Information Security Manager (CISM),
  - o Certified Information Systems Auditor (CISM),
  - o Certified in Risk and Information Systems Control (CRISC);
- Microsoft (https://www.microsoft.com/en-us/learning/mcse-cloud-platform-infrastructure.aspx) (MS Office Suite, enterprise networking, server technologies, business application development, databases, software development, cloud computing):
  - o Microsoft Office Specialist (MOS),
  - o Microsoft Certified Solutions Developer (MCSD),
  - o Microsoft Certified Solutions Expert (MCSE),
  - o MCSE: Cloud Platform and Infrastructure;
- VMWare (https://www.vmware.com) (cloud computing):
  - o VCP6 – DCV.

The most valuable certifications (White and Hein, 2017) also cover project management area since IT professionals in management positions often seek these certifications:

- Project Management Institute (https://www.pmi.org) (PMI) (project management):
  - o Certified Associate in Project Management (CAPM),
  - o Project Management Professional (PMP);
- SCRUM (https://www.scrumalliance.org/certifications/practitioners/certified-scrummaster-csm) (agile project management):
  - o Certified Scrum Master (CSM).

Table 2 shows the U.S. organizations that are already established and well known in the IT market, according to IT literature, that offer education, training and certification in information technology and security on global worldwide scale. The list contains also organizations outside of the USA, from Europe – United Kingdom, Netherlands, and Belgium and from Asia – Singapore. Table 2 lists the names, the focus of the organization's offerings (education/training; certification), web address, geographical availability/scope, credentials, country of origination, and type (private-public; for-profit, not-for-profit). The organizations offer variety of professional certifications at various levels: entry, professional, and master.

Table 3 lists the organizations, mostly located in the USA, and their respective certification programs'

Table 2. Organizations offering education, training, and/or certifications in the area of information technology, computer networks, and security worldwide mostly at professional level in the USA and elsewhere

Organization/ /Entity Name	Focus A-Accreditation E-Education/ Training C-Certification	Web address	Availability/ Scope	Credentials: Approved /Recognized/ Endorsed by	Country/ Established	Type Public/Private For-profit /Non-profit
Computer Technology Industry Association (CompTIA)	C- basic, professional, master	www.comptia.org	Global (120 countries)	IT Industry recognition U.S. ANSI; Cybersecurity-U.S. DoD	USA/1982	Non-profit
Cisco Systems	C-professional	www.cisco.com	Global	IT Industry	USA/1984	For-profit
CREST	A&C	www.crest-approved.org	Global	IT Industry	UK/2006	Non-profit
DRI International	E&C	www.drii.org	Global	IT Industry	USA/1988	Non-profit
The International Council of Electronic Commerce Consultants (EC-Council)	C-Cybersecurity professional certification	www.eccouncil.org	Global (over 87 countries)	U.S. Agencies endorsement; CNSS	USA/2001	For-profit
The European Information Technologies Certification Institute (EITCI)	E-Digital literacy; C-Information Communication Technologies	eitci.org	Global	IT Industry	Brussels/ Belgium 2008	Non-profit

Table 2 – cont.

Organization/ /Entity Name	Focus A-Accreditation E-Education/ Training C-Certification	Web address	Availability/ Scope	Credentials: Approved /Recognized/ Endorsed by	Country/ Established	Type Public/Private For-profit /Non-profit
Global Information Assurance Certification (GIAC)	C-IT, Computer Security	www.giac.org	Global	IT-Industry	USA/ GIAC 1999	Private; for profit
The International Association of Computer Investigative Specialists (IACIS)	E C-Computer Forensics	www.iacis.com	Global	IT Industry	USA/1990	Non-profit
International Association of Privacy Professionals (IAPP)	E C	aipp.org	Global (83 countries)	IT Industry	USA/2000	Non-profit
IEEE Computer Society	E & C	www.computer.org	USA	IT Industry	USA	Non-profit
EXIN	E & C – IT	www.exin.com	Global (165 countries)	IT Industry	Netherlands	For-profit
Information Systems Audit and Control Association (ISACA)	Auditing Controls in Computer Systems	www.isaca.org	Global	IT Industry	USA/1967	Non-profit
The International Information System Security Certification Consortium (ISC)²	E & C-Information Security Professional	www.isc2.org	Global	U.S. DoD; NIST, ANSI/ISO/IEC 17024 IT Industry	USA/1989	Non-profit
International Society of Forensic Computer Examiners (ISFCE)	T & C	www.isfce.com	Global	IT Industry	USA/2003	Private
Microsoft	E & C	www.microsoft.com	Global	IT Industry	USA/1975	For-profit
Mile2	C-Cybersecurity Infrastructure Security Professional	www.mile2.org	Global	U.S. NSA, CNSS (4013)	USA/1992	Private
The National Infocomm Competency Framework (NICF)	E&C-(through partners) IT, Security	portal.imda.gov.sg/sub/nicf	Singapore	IT Industry	Singapore/ unknown	Quasi-Governmental
Offensive Security	E&C	www.offensive-security.com	Global	IT Industry	USA/2003	For-profit
Software Engineering Institute (SEI) CERT program	E&C	www.sei.cmu.edu www.cert.org	Global	IT Industry	USA/1984	Sponsored by U.S. DoD

Source: IT literature.

Table 3. Organizations offering certifications in information technology, computer networks, and cybersecurity

Granting Entity	Topic	Certification
CompTIA	Computer Networks, Security	CompTIA Security+, CompTIA Advanced Security Practitioner (CASP) Cloud (2011)
Cisco Systems	Computer Networks, Security	CCENT CCNA Security CCNP Security CCIE Security CCSE Security Engineer
CREST	Information Security	CREST Registered Penetration Tester
DRII	Disaster Recovery	Certified Business Continuity Professional (CBCP)
EC-Council	E-business & Information security	Certified Ethical Hacker (CEH) Computer Hacking Forensics Investigator (CHFI) EC-Council Certified Security Analyst (ECSA) License Penetration Tester (LPT)
EITCI	Information and Communication Technologies, Security	• European Information Technologies Certification Academy EITCA/IS certifications
EXIN	IT	• Variety of IT certifications
GIAC	Information security	Certified Incident Handler (CIH) Certified Information Systems Security Professional (CISSP) Certified Penetration Tester (GPEN) Certified Incident Handler (GCIH) Information Systems Security Management Professional (ISSMP) Information Systems Security Engineering Professional (ISSEP) • Information Systems Security Architecture Professional (ISSAP) • GIAC Security Expert (GSE) Systems Security Certified Practitioner (SSCP)
IACIS	Computer Forensics	Certified Forensic Computer Examiner (CFCE) Cyber Incident Forensics Response Mobile Device Forensics
IAPP	Information Security & Management	Certified Information Privacy Professional (CIPP) Certified Information Privacy Manager (CIPM)
IEEE & NotSoSecure	Cybersecurity	Art of Hacking
ISACA	Information security	• Certified Information Systems Auditor (CISA) • Certified Information Security Manager (CISM) • Certified in Risk and Information System Control (CRISC)
ISC^2	Information security	Certified Information Systems Security Professional (CISSP) Systems Security Certified Practitioner (SSCP) Information Systems Security Management Professional (ISSMP) Information Systems Security Engineering Professional (ISSEP) Information Systems Security Architecture Professional (ISSAP)
ISFCE	Computer Forensic	Certified Computer Examiner (CCE)
Microsoft	Networking & Security	Networking Fundamentals Security Fundamentals among others
Mile2	Cybersecurity	Certified Information Systems Security Auditor (CISSA) Certified Information Systems Security Officer (CISSO) Certified Information Systems Security Manager (CISSM) Certified Penetration Testing Engineer/Examiner (CPTE) Certified Professional Ethical Hacker (CPEH)
NICF	Information Technology, Security	Variety certifications via partners
Offensive Security	Information Security	Offensive Security Certified Professional (OSCP) Offensive Security Exploitation Expert (OSEE)
SEI CERT	Computer Security	Computer Security Incident Handler (CSIH)

Source: Dickson, 2016; Tittel, 2016, IT literature.

topics or themes and the names of the offered specific certifications that cover computer networks and information security (Dickson, 2016; Tittel, 2016; IT literature). Many of these certifications are most sought after by professionals seeking to upgrade their knowledge and skills set as a job requirement or to advance their careers (Dickson, 2016; Tittel, 2016; IT literature). The mentioned organizations offer other educational, training programs, and certifications, in broadly understood information technology field outside of the topical focus of this paper as well.

The abbreviations used in Table 2 and Table 3 stand for:

- The CNSS is a federal government entity under the U.S. Department of Defense (DoD) that provides procedures and guidance for the protection of national security systems.
- ANSI American National Standards Institute, private non-profit organization (www.ansi.org) oversees the development of voluntary consensus standards for products, services, processes, and systems in the USA. It coordinates U.S. standards with international standards.
- CERT Center of Internet Security Expertise, established by U.S. Department of Defense in 1988, administrated by Carnegie Mellon University.
- SANS stands for SystAdmin, Audit, Network and Security.
- NICF The National Infocomm Competency Framework is a national Singapore quasi-government platform that helps information technology and communication professionals and employers to determine the types of skills and competencies required for various information technology and communication jobs and develop training strategies to acquire these skills.

Industry Top-Tier Certifications in Information Security

Information security and especially cybersecurity became an area of high demand for professionals in the light of Internet's dramatic rise in use and applications. According to Tittel (2016), "in 2016 there were more than 200,000 information security position available in the USA, with forecasts pointing to 1.5 million open positions globally by 2019." Cybersecurity which encompasses computer networks and systems' vulnerability and penetration testing, breach detection, secure coding, attack mitigation (Dickson, 2016) is the subject of numerous certifications in the USA and abroad. The list below contains the names of the most sought after certifications (Dickson, 2016; Lindros, 2016; Tittel, 2016; IT literature):

- CompTIA Security+ by CompTIA (https://certification.comptia.org),
- CCNA, CCNP, CCIE Security by Cisco Systems (http://www.cisco.com),
- CEH: Certified Ethical Hacker and ECSA: Certified Security Analyst both by EC-Council (https://www.eccouncil.org),
- CFCE: Certified Forensic Computer Examiner by IACIS (http://www.iacis.org),
- GSEC: SANS GIAC Security Essentials by GIAC (www.giac.org),
- CISSP: Certified Information Systems Security Professional by (ISC^2, http://isc2.org),
- CISA: Certified Information Systems Auditor and CISM: Certified Information Security Manager both by ISACA (https://www.isaca.org).

The certifications cover IT tools, current techniques and methodologies, and best practices as established and demanded by information technology and security areas. The organizations offer various certifications and some of them also training mostly of 1-week or 2-weeks in duration of intensive courses that combine theory with practice on computer technologies including security theme at basic, professional, and advanced level.

In the next section the most sought after certifications, their scope and contents will be described in more detail.

Computing Technology Industry Association (CompTIA)

CmpTIA (https://certification.comptia.org) is a non-profit trade association organization representing the information technology industry. The organization is the leading supplier of vendor-neutral IT certification worldwide. The CompTIA has developed education, training, and certification exams for computing support, networking, security, open-source (Linux) development, and cloud and mobile applications. In the area of computer security CompTIA Security+ certificate is a globally recognized and trusted certificate that covers the essentials of computer networks security and risk management, cryptography, identity management, and security systems. CompTIA recommends at least two years of administrative experience and prior passing of its CompTIA Network+ certification. CASP certification is designed to give an advanced-level security skills and knowledge for which at least ten years of IT administration with five years of technical security experience is required. These certifications have been approved by U.S. Department of Defense (Directive 8570/8140). Recently CompTIA also obtained an ISO 17024 certification.

It is worth mentioning that CompTIA is one of an increasing number of organizations, listed in the subsequent section, that are currently offering certification in the area of cloud computing services.

The list below provides current CompTIA (https://certification.comptia.org) offering of certifications at various levels from entry level – fundamental, through specialty, to professional/mastery:

- Foundational Level: IT Fundamentals,
- Specialty Level: CDIA+, CTT+, Cloud Essentials,

- Professional Level: A+, Network+, Cloud+, Project+, CSA+, Security+, Linux+, Server+, Mobility+,
- Mastery Level: CASP (CompTIA Advanced Security Practitioner).

Cisco Systems (http://www.cisco.com)

Well established Cisco certifications offer CCNA at associate level, CCNP Security at professional, and CCIE Security at expert levels. Although there is no formal pre-requisites, Cisco recommends accruement of minimum three years of in-depth pertinent job experience prior to taking exams.

The International Council of E-Commerce Consultants (EC-Council)

The International Council of E-Commerce Consultants (EC-Council, https://www.eccouncil.org) as a member-based organization, is the world's largest cybersecurity technical certification entity that certifies individuals in various e-business and information security knowledge and skills. The organization offers Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI) and EC-Council Certified Security Analyst (ECSA)/License Penetration Tester (LPT) certifications as well as many others certifications that are offered in over eighty seven countries globally. CEH appears continuously as one of the top certifications. Certification obtained accreditation from the American National Standards Institute (ANSI).

International Association of Computer Investigate Specialists (IACIS)

The International Association of Computer Investigate Specialists (IACIS, http://www.iacis.org) is a non-profit organization founded in 1990 that offers mostly 2-week intensive courses in various areas at essential, basic and advanced levels. Among others, IACIS offers specialized training for Certified Forensic Computer Examiner (CFCE) and *Cyber Incident Forensic Response* (CIFR) certifications.

Global Information Assurance Certification (GIAC)

GIAC (www.giac.org) is a private organization of global scope. GPEN and GCIH by GIAC are professional certifications with GIAC Security Expert (GSE) being at the top, mastery level. The GIAC does not require any formal specific training for any of its certifications exams but recommends relevant job experience before taking one. GIAC certifications were approved for DoD information assurance.

The International Information System Security Certification Consortium (ISC^2)

ISC^2 (ISC^2, http://isc2.org) is a global non-profit organization which offers a variety of certifications at professional level. Its top certification is CISSP: Certified Information Systems Security Professional designed for security managers, directors of information and system security, network architects, etc. ISC^2 was the first information security certifying organization to meet the requirements of ANSI/ISO IEC Standard 17024 (http://www.cyberdegrees.org).

IEEE Computer Society & NotSoSecure (UK firm)

IEEE Computer Society (http://www.computer.org) together with NotSoSecure UK firm started to offer the Art of Hacking course and certification in March, 2016. The course is comprised of Web and infrastructure hacking training, with 25 percent e-learning and 75 percent online labs. The course and certification which are designed at an advanced level, each must be completed within 6 months upon commencement.

ISACA

ISACA (https://www.isaca.org), formed in 1969, is a global non-profit organization offering certifications and practical guidance and effective tools in information systems. Its certifications: CISSP and CISM are designed for professionals in management-level assignments who oversee and assess an enterprise's information security design and implementations. The jobs may include: governance, risk management and compliance, and incident management.

There are no public domain publications available, known to author, that state total numbers of certifications granted in the IT areas of computer networks, information security, or cloud computing. One can cite the numbers reported by organizations themselves that offer IT certifications. EXIN (www.exin.com) reports, for example, over 2 million professionals certified with its various IT certificates worldwide. Another organization (ISC^2, http://isc2.org) claims that its highly respected by IT community but a narrower in scope Certified Information Systems Security Professional (CISSP) certification is held by 112,412 professionals worldwide in 163 countries. It is reported (https://www.techopedia.com/definition/24747/cybersecurity) that CompTIA (http://www.cisco.com), another certification organization, certified over 2.2 million IT professional worldwide with its various certifications since its inception in 1982. Some organizations including CompTIA (http://www.cisco.com) are changing or contemplating changing their policies with regard to expiration dates of their certificates and limiting them to, for example, 3 or 5 years, which is understandable in the light of fast changing IT field.

Organizations Offering Certifications in Cloud Computing

An increasing role played by cloud computing (cc) in today's business operations and environment warrants a separate listing and description of organizations offering cc certifications. Table 4 lists the names of organizations offering cloud computing certifications with their web addresses, type of certifications (vendor-neutral, VN; or vendor-specific, VS), and the names of certifications. Most of the listed organizations

Table 4. Organizations offering cloud computing certifications (alphabetical order)

Granting Entity	Address	Country	VN/VS	Certification/Exam Names
Amazon	www.amazon.com	USA	VS	AWS Certified Solutions Architect
Cisco Systems	www.cisco.com	USA	VN & VS	CCNA Cloud CCNP Cloud
Cloud Security Alliance (CSA)	cloudsecurityalliance.org	USA	VN	Certificate of Cloud Security Knowledge
Cloud Credential Council	www.cloudcredential.org	USA	VN	Cloud Technology Associate Professional Cloud Administrator Professional Cloud Solutions Architect
Cloud Genius	be.a.cloudgeni.us	USA	VN	Cloud Technologies Cloud DevOps Cloud Architecture and Design
Cloud Institute	Cloud-institute.org	USA	VN	Certified Cloud Architect Certified Cloud Professional
CloudSchool	CloudSchool.com	USA	VN	Certified Cloud Professional Certified Cloud Architect Certified Cloud Security Specialist
Comp TIA	www.comptia.org	USA	VN	CompTIA Cloud Essentials CompTIA Cloud +
Dell	www.dell.com	USA	VS	Dell EMCCA EMC Cloud Architect
Exin	www.exin.com	Netherlands	VN	Cloud Computing Foundation Cloud Technologies Advanced
Google	www.google. com	USA	VS	Google Certified Cloud Architect
IBM	www.ibm.com	USA	VS	IBM Certified Cloud Solution Architect
Microsoft	www.microsoft.com	USA	VS	MSCE: Cloud Platform and Infrastructure MCSA: Cloud Platform MCSA: Linux on Azure Exams: – Cloud Fundamentals – Configuring and Developing a Private Cloud – Architecting Microsoft Azure Solutions – Designing and Implementing Cloud Data Platform Solutions – Developing Microsoft Azure and Web Services – Configuring and Operating a Hybrid Cloud with Microsoft Azure Stack – Perform Cloud Data Science with Azure Machine Learning among others
Rackspace	www.rackspace.com	USA	VN	CloudU
Red Hat	www.redhat.com	USA	VS	System Administrators in Red Hat OpenStack
Salesforce	www.salesforce.com	USA	VS	Salesforce Certified Technical Architect among others
VMware	www.vmvare.com	USA	VS	VMware VCP6-Cloud

Source: Tittel and Kyle, 2017; Florentine, 2017; IT literature.

provide certifications on global worldwide scale, at foundational, associate and expert levels. Majority of these organizations do provide educational material and/or training for the purpose of certification.

Among the listed certifications in Table 4 the following five are the most sought after (Tittle and Kyle, 2017) (in alphabetical order):

- Amazon (http://www.amazon.com): AWS Certified Solutions Architect,
- Cisco (http://www.cisco.com): CCNA Cloud, CCNP Cloud,
- Dell (https://education.emc.com/content/emc/en-us/home.html): EMCCA EMC Cloud Architect,

- Microsoft (https://www.microsoft.com/en-us/learning/mcse-cloud-platform-infrastructure.aspx): MCSE Cloud Platform and Infrastructure.

University/College Programs and Certificates

Information security in the context of computer networks has been incorporated as part of the content in standard course offerings at universities and colleges in the information technology and science and computer science programs across the USA and worldwide for last twenty years. However, it attained its deserved attention as a separate discipline only relatively recently in last decade. Many universities and colleges, to meet the growing demand for information security professionals decided to expand their programs and offer new programs at undergraduate and graduate levels and also to offer certification programs either at campus location or online. The certifications are designed for professionals who desire to augment their knowledge and skills set and/or expand their career opportunities. A compendium of information about various programs and certifications can be accessed at http://www.cyberdegrees.org. The program and certification offerings are at undergraduate and advanced, graduate levels. In this section a few examples of such offerings will be described.

Undergraduate certificate in Security and Risk Analysis (SRA) – Penn State University

The SRA certificate is offered via Penn State World Campus (http://www.worldcampus.psu.edu/degrees-and-certificates/security-risk-analysis-certificate/overview), that offers variety of programs online (www.worldcampus.psu.edu). The certificate requires 15 credits to be completed in programming (CMPSC 101, 121) or application development (IST 140); technology, security and risk analysis (IST 110, SRA 111), terrorism and crime, information security (SRA 211, 221). The certification also counts toward the bachelor degrees in IST or SRA.

IST Cybersecurity Analytics and Operations Bachelor Degree – Penn State University

Penn State College of Information Sciences and Technology (IST) (https://ist.psu.edu/students/undergrad/majors/cybersecurity) will offer a new degree program that meets the demand for information security professionals beginning in the spring 2018. The program will provide three key areas of expertise: technical cyber defense strategies, risk management, and data-driven cybersecurity analytics. IST College being already a designated Center of Academic Excellence in Cyber-Defense Education by the U.S. National Security Agency and Department of Homeland Security, by offering of a new program expands its offerings in information security field. The program is "one of the first of its kind in the nation" according to the program creators. This program is an example of how universities respond to new needs of the national economy.

Computer Networking Undergraduate Certificate – University of Maryland (http://www.umuc.edu)

The offering is similar to described above plan by Penn State University – it requires 18 credits in fundamentals of computer troubleshooting and networking (CMIT 202, CMIT 265), network security (CMIT 320), configuring Cisco devices (CMIT 350), installing Windows Server (CMIT 369), and upper level CMIT elective. The credits can be applied toward bachelor degree. (Here, CMIT=Computer Management Information Technology.)

Master of Science in Cybersecurity (M.S. in Cybersecurity), Delivered Online – Syracuse University

The master degree offered by Syracuse University (https://engineeringonline.syr.edu/graduate-programs/cybersecurity/), Engineering and Computer Science Department, is delivered online and it prepares students to identify, prevent, and counteract cybercrime (www.syr.edu). Curriculum focuses on: design and protection of systems, analysis and detection of malware and anomaly, and data mining. It requires 30 credits to be completed within 15 months.

Certificate in Cybersecurity Strategy – Georgetown University (https://scs.georgetown.edu/)

The enrollee must successfully complete six required courses in: cybersecurity, threats, vulnerabilities, crisis and security management, and countermeasures and risk assessment. The program is offered on campus and online, and requires bachelor degree and 3–5 years of professional experience in the field.

Graduate Certificate in Network Security – University of Massachusetts at Lowell (http://www.uml.edu)

This is graduate level certificate program for professionals who wish to advance their knowledge and skills in advanced-level studies in information technology. The program is offered online and consists of four courses in: network security, digital forensics, network infrastructures, and mobile networks. The certification can be counted toward Master Degree in Information Technology.

Advanced Computer Security Certificate – Stanford University

Stanford Advanced Computer Security Certificate (https://computersecurity.stanford.edu) gives advanced skills in protecting networks, prevent cyberattacks, and building secure infrastructures. The program consists of six online computer science courses (three required and three electives): Software Security Foundations (XACS101), Mobile Security (XACS215), Using Cryptography Correctly (XACS130), Writing Secure Code (XACS 131), Exploiting and Protecting Web

Applications (XAC133), Network Security XACS255, Emerging Threats & Defenses (XACS301). The program is designed for "busy" professionals of cybersecurity workforce.

SEI Certification – Carnegie Mellon University

The Software Engineering Institute (SEI, https://www.sei.cmu.edu/certification), a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD), and operated by Carnegie Mellon University provides education, training, SEI authorization, and certification. Certifications provided by SEI cover variety of topics; in the area of cybersecurity Institute offers: Computer Security Incident Handler and Insider Threat Vulnerability Assessor.

Free Online Cybersecurity Courses via Massive Open Online Courses Platform (MOOCs)

Massive Open Online Courses (MOOCs, http://www.cyberdegrees.org/resources/free-online-courses/) are offered by a variety of universities and colleges around the country. They are being offered at both undergraduate and graduate levels. While some are available at the amateur level, some other do require certain more advanced skills. The courses usually take 6–10 weeks to complete and involve variety of assessment methods: from peer-to-peer evaluations, class discussions, hands-on projects, programming labs, and exams. Examples of schools which offer such MOOC courses are: University of Michigan (Introduction to Cyber Security), University of Washington (Designing and Executing Information Security Strategies), University of Maryland (Cybersecurity Specialization, Cryptography, and Hardware Security), and MIT (Cryptography, Network and Computer Security). There are a few non-profit organizations that offer MOOC courses such as Udacity (https://en.wikipedia.org/wiki/Udacity), which originated with free classes offered by Stanford University in 2011 and now has big U.S. corporations, AT&T for example, as partners. The initial focus of Udacity (https://en.wikipedia.org/wiki/Udacity) on university-type courses has changed to vocational education for professionals. In 2014 Georgia Institute of Technology launched its online computer science degree in partnership with Udacity and AT&T Corporation although with some costs to students. Set up by Harvard University and MIT in 2012 edX (https://www.edx.org) is another example of an organization offering MOOC courses. A nonprofit and an open-source MOOC provider, edX, has a global reach worldwide with 90 global partners already including MIT. MIT's MOOC courses delivered via edX platform are referred to as MITx. Coursera (https://www.coursera.org) is another example of an organization providing MOOC with extensive offering of 2,545 courses and global partners across 29 countries.

With such increasing popularity and enrollment numbers the question arises: what are the MOOC courses completion rates? The reported numbers are extremely low. Some reported 90 percent or above dropout rates. In one example of the MOOC course offered by Coursera, Rivard (2013) reported that "only about 350 of the 12,700 or so Coursera users who registered for the course took the final exam, a dropout rate of 97 percent." The U.S. National Science Foundation funded activities (Rivard, 2013) to study the MOOC users that, it is hoped, would lead into improving the dropout rates. Some already suggest to change enrollment policies and to introduce enrollment fees. There are also opinions that the classic measurements regarding dropout rate are wrong and there should be other metric used since mostly nontraditional students enrolled in MOOC courses may have other objectives in mind by enrolling such as, for example, satisfying only curiosity about subject matter without going into depth. Furthermore, "window shoppers and false starters" as they constitute a significant portion of initial MOOC enrollees, reaching 26 percent Clark (2016) notes, should not be counted to begin with.

It seems that further pedagogical experimentations and investigations of content delivery methods in conjunction with admission standard policies are in order to address effectively the above listed MOOCs' concerns.

Certificate at Penn State – Fayette in Computer Networks, Cybersecurity, and Cloud Computing

The growing number and variety of computer security threats, including identity theft, have led to an increased interest in computer and computer network security issues and consequently resulted in new programs, courses, and certification offerings by academic institutions. The purpose of this section is to describe the activities and content of the certificate in Computer Networks and Security under development at Penn State – Fayette to meet a growing local demand in information technology for skilled workforce.

While computer networks and security have been a subject of already extensive literature which provided theoretical and practical foundations of the academic programs (Beasley and Nilkaew, 2012; Boyd and Proudfoot, 2014; Kizza, 2013; Palmer, 2008; Schou and Shoemaker, 2007; Solomon and Chapple, 2005; Velte and Velte, 2013; and Weidman, 2014, among others), the purpose of the training and certification programs offered by various organizations, mostly outside of academia, is to offer current practical knowledge and expertise to professionals in narrow usually specialties.

The author's interest in the computer networks and information security issues resulted in various publications (see references; Sokol and Gapinski, 2002) and in his involvement in a certificate initiative. Namely, the author presently is engaged in the developing of the certificate program in the area of computer networks, security, and cloud computing services as reported already at WEEF'2016 conference (Gapinski, 2016b). The certificate program under development will cover the essential concepts of computer networks (peer-to-peer and client/server local area networks (LANs), wide-area networks (WANs) technologies, including: planning, installation, server configuration, resource management, remote access, performance monitoring, and optimization; security (malware, attack tactics, data security, cryptography, wireless/mobile security, authentication/access techniques); and cloud computing (definition, classification, types, standards, vulnerabilities, virtualization and virtual machines including Hyper-V, security, and services: IaaS/PaaS/SaaS). It is planned that the program will offer threat simulations based on the Microsoft Windows and open source Linux platforms.

The certificate will include the technical elective courses, under development, in cybersecurity and cloud computing which will also serve as technical electives in various campus's academic majors including EET/ENG/IST/AOJ programs.

Laboratory exercises will cover the following subjects:

- Operating systems and Networking:
  - o MS Windows and Linux environments,
  - o Basic concepts of networking: topologies, protocols, packet switching, routing,
  - o Server – client services (Email service, Web server);
- Cybersecurity:
  - o Information Security,
  - o Cryptography,
  - o Intrusion Detection,
  - o Virtual penetration,
  - o Denial-of-Service Attacks;
- Cloud services:
  - o Vulnerabilities related to cloud computing services,
  - o Creating a VM using Amazon AWS EC2,
  - o Using Microsoft MS Azure,
  - o Storage in cloud,
  - o Infrastructure as IaaS – cloud computing security (using Apache CloudStack and OpenStack open source cloud middleware systems);
- Data Backup and Recovery.

It is planned that the certificate contents will be delivered in a hybrid format, which combines online delivery of lectures' topics and on campus execution of laboratory assignments.

Conclusions

The goal of this article was to overview the certification programs in networking, security, and cloud services that are offered currently in the USA and elsewhere. As IT area expands its omnipresence to almost all aspects of business operations, the importance of certifications programs will only increase to advance one's knowledge and skills set or advance one's career. To meet current and future demand for IT professionals, many professional organizations and institutions of higher education such as universities and colleges are involved in offering of certificates at various depths: from introductory to expert, from undergraduate to graduate levels. Most of IT organizations or companies offering certifications originated in the USA and have already global scope providing their services worldwide. Numerous organizations, in addition to certifications, do provide extensive educational and training sessions of various lengths in both resident and online formats. Various organizations have either accreditation or endorsement from leading industry peers and/or national or international certification.

An example of such a certificate program pursued at PSU-Fayette is described. The certificate will be offered to IT professionals, business, and engineering personnel for a variety of local industrial and service oriented firms, which may include manufacturing, high-tech, and healthcare.

References

Amazon, http://www.amazon.com.

Balakrishnan, V. (2010). *Trust Enhanced Security Framework For Mobile Ad Hoc Wireless Networks*. Sydney: Ph.D. Thesis. Dept. of Computing. Macquarie University.

Beasley, J., & Nilkaew, P. (2012). *Networking Essentials.* 3rd ed. Indianapolis: Pearson Education.

Boyd, R. & Proudfoot, J. (2014). *Applied Information Security, a Hands-on Guide to Information Security Software.* New York: Prentice-Hall.

Cisco, http://www.cisco.com.

Clark, D. (2016). *MOOCs: Course Completion is the Wrong Measure of Course Success*. Retrieved from https://www.class-central.com/report/moocs-course-completion-wrong-measure/).

Claycomb, W.R. (2012). *Tutorial: Cloud Computing Security*, Retrieved from https://resources.sei.cmu.edu/asset_files/Presentation/2012_017_001_52439.pdf.

CompTIA, https://certification.comptia.org.

Coursera, https://www.coursera.org.

Cyberdegrees, http://www.cyberdegrees.org.

DELL EMC, https://education.emc.com/content/emc/en-us/home.html.

Dickson, B. (2016). *10 Hot Cyber Security Certifications for 2017*. IT Career Finder. Retrieved from https://www.itcareerfinder.com/brain-food/blog/entry/10-hot-cyber-security-certifications-for-2017.html.

edX, https://www.edx.org.

EITCI European Information Technologies Certification Institute, http://eitci.org.

EXIN, https://www.exin.com.

Florentine, S. (2017). *The most valuable cloud computing certifications today*. Retrieved from https://www.cio.com/article/3207553/certifications/the-most-valuable-cloud-computing-certifications-today.html.

Fortinet (2017). *Mapping the Ransomware Landscape*. Retrieved from https://www.fortinet.com/demand/gated/mapping-ransomware-landscape.html.

Gapinski, A. (2003). *A Note on LAN, ATM Technologies, and Priority Queuing*. Proceedings of International Conference on Industry, Engineering & Management Systems (IEMS). Florida. 515–519.

Gapinski, A. (2005). *A Note on Teaching Cisco Routers*. Proceedings of IEMS'2005. Florida. 137–141.

Gapinski, A. (2014). Strategies for Computer Networks' Security. *Business Administration Quarterly*, *32*(3), 59–65. Retrieved from https://przedsiebiorstwo.waw.pl/resources/html/article/details?id=59512.

Gapinski, A. (2015). *Cloud Computing: Information Security Standards, Compliance and Attestation*. Proceedings of International Conference on Engineering and Technologies (LACCEI). Santo Domingo. Retrieved from www.laccei.org.

Gapinski, A. (2016a). Cloud Computing Services: Status and Trends. *e-mentor*, *64*(2), 70–78. http://dx.doi.org/10.15219/em64.1241

Gapinski, A. (2016b). *Developing a Certificate Program in Computer Networks Technologies, Security, and Cloud Computing Services*. Proceedings of World Engineering Education Forum (WEEF) Conference. Seoul.

Gapinski, A. (2017). Automation and its Effect on STEM Occupations. Economic and Ethical Impact. *Research in Logistics and Production*. *7*(5), 391–407. http://dx.doi.org/10.21008/j.2083-4950.2017.7.5.1

Georgetown University School of Continuing Studies, https://scs.georgetown.edu/.

Global Information Assurance Certification (GIAC), http://www.giac.org.

Grobauer, B., Walloschek, T., & Stöcker, E. (2011). *Understanding Cloud Computing Vulnerabilities*. IEEE Computer and Reliability. IEEE Security & Privacy, March/April 2011. http://doi.ieeecomputersociety.org/10.1109/MSP.2010.115

Half, R. (2017). *Which IT certification are most valuable?* Retrieved from https://www.roberthalf.com/blog/salaries-and-skills/which-it-certifications-are-most-valuable.

Harfoushi, O., Alfawwaz, B., Ghatasheh, N., Obiedat, R., Abu-Faraj, M., & Faris, H. (2014). Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review. *Communications and Network*, *6*(1), 15–21. http://dx.doi.org/10.4236/cn.2014.61003

Homeland Security (2017). *Cybersecurity Questions for CEOs*. Retrieved from https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf.

IACIS International Association for Computer Information Systems, http://www.iacis.org.

IDC Enterprise Panel (August 2008).

IEEE Computer Society, http://www.computer.org.

Information Systems Audit and Control Association (ISACA), https://www.isaca.org.

Kizza, J.M. (2013). *Guide to Computer Network Security*. Springer-Verlag. London.

Lindros, K. (2016, December 28). 5 Great 'Starter' Cybersecurity Certifications. *Business News Daily*. Retrieved from http://www.businessnewsdaily.com/9661-cybersecurity-certifications.html.

Massive Open Online Courses, http://www.cyberdegrees.org/resources/free-online-courses/.

Merriam-Webster, https://www.merriam-webster.com/dictionary/ransomware.

Microsoft, https://www.microsoft.com/en-us/learning/mcse-cloud-platform-infrastructure.aspx.

National Infocomm Competency Framework NICF, https://www.imda.gov.sg/industry-development/programmes-and-grants/individuals/national-infocomm-competency-framework-nicf.

Pak, Ch. (2017). *Cloud Security*. IEEE Computer Society. Webinar.

Palmer, M. (2008). *Hands-On Microsoft Windows Server 2008*. Boston: Course Technology, Cengage Learning.

Penn State College of Information Sciences and Technology, https://ist.psu.edu/students/undergrad/majors/cybersecurity.

Penn State World Campus, http://www.worldcampus.psu.edu/degrees-and-certificates/security-risk-analysis-certificate/overview.

PMI, https://www.pmi.org.

Ristenpart, T., Tromer, E., Shacham, H., and Savage, S. (2009) *Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds.* Proceedings of the 16 ACM Conference (CCS'09). Chicago. 199–212.

Rivard, R. (2013). *Measuring the MOOC Dropout Rates*. Inside Higher Education. March 8. Retrieved from https://www.insidehighered.com/news/2013/03/08/researchers-explore-who-taking-moocs-and-why-so-many-drop-out.

Schou, C., & Shoemaker, D. (2007). *Information Assurance for the Enterprise. A Roadmap to Information Security.* New York: McGraw-Hill.

SCRUM, https://www.scrumalliance.org/certifications/practitioners/certified-scrummaster-csm.

Software Engineering Institute, https://www.sei.cmu.edu/certification/.

Sokol, J., & Gapinski, A. (2002). *Creating a Course In Computer Networking: Electrical Engineering Technology Versus Information Science and Technology*. Proceedings of International Conference on Industry, Engineering & Management Systems (IEMS). Florida. 7–11.

Solomon, M.G., & Chapple, M. (2005). *Information Security Illuminated.* Sudbury, Massachusetts: Jones & Bartlett Publishers.

Stanford University, https://computersecurity.stanford.edu.

Stolfo, S.J., Bellovin, S.M., Hershkop, S., Keromytis, A.D., Sinclair, S., & Smith, S.W. (Eds). (2008). *Insider Attack and Cyber Security: Beyond the Hacker.* Springer-Verlag, Advances in Information Security 39.

Syracuse University of Engineering and Computer Science. https://engineeringonline.syr.edu/graduate-programs/cybersecurity/.

Techopedia, https://www.techopedia.com/definition/24747/cybersecurity.

The Convergence of Operational Risk and Cyber Security (2016). Retrieved from https://www.accenture.com/t20170803T055319Z__w__/us-en/_acnmedia/PDF-7/Accenture-Cyber-Risk-Convergence-Of-Operational-Risk-And-Cyber-Security.pdf.

The International Council of Electronic Commerce Consultants (EC-Council), https://www.eccouncil.org.

The International Information System Security Certification Consortium (ISC), http://isc2.org.

Tittel, E. (2016). *Best Information Security Certifications For 2017*. Tom's IT PRO. Retrieved from http://www.tomsitpro.com/articles/information-security-certifications,2-205.html.

Tittel, E., & Kyle, M. (2017). *Best Cloud Certifications*. Tom's IT PRO. Retrieved from http://www.tomsitpro.com/articles/cloud-it-certifications,2-537.html.

Umass Lowell, http://www.uml.edu.

University of Maryland University College, http://www.umuc.edu.

U.S. Dept. of Labor. Bureau of Labor Statistics, https://www.bls.gov.

Velte, T., & Velte, A. (2013). *Cisco: A Beginner's Guide.* 5th ed. New York: McGraw-Hill.

Weidman, G. (2014). *Penetration Testing: A Hands-On Introduction to Hacking.* 2nd ed. San Francisco: No Starch Press.

White, S.K., & Hein, R. (2017). *The 13 most valuable IT certifications today*. Retrieved from https://www.cio.com/article/2392856/it-skills-training/careers-staffing-12-it-certifications-that-deliver-career-advancement.html.

Wikipedia, https://en.wikipedia.org/wiki/List_of_computer_security_certifications.

Wikipedia, https://en.wikipedia.org/wiki/Udacity.

Certificate Programs in Computer Networks, Security, and Cloud Computing in the USA – A Review

The objective of the article is to review certificate programs in computer networks and computer security which are currently offered by many educational institutions and various organizations in the USA. Due to an increased role played by computer networks and cybersecurity, the certificate programs' contents and scopes are being augmented to incorporate new area of interest such as cloud computing and its services to meet market expectations and demands. The article describes new cybersecurity threats posed by the growing use of cloud computing services and the related cloud computing certification programs. An analysis of the certifications held by U.S. workforce including STEM occupations is provided. The article presents an analysis of the certificate programs' offerings and their contents that are offered by various public as well as private organizations and institutions including higher education. The article, in addition, describes the author's activities while developing the certificate program in the area of computer networks, cybersecurity, and cloud computing currently under consideration at The Pennsylvania State University – Fayette Campus.

Andrzej J. Gapinski, Ph.D. is an Associate Professor of Engineering at The Pennsylvania State University, Pennsylvania, USA. Dr. A. Gapinski received his Ph.D. in Electrical Engineering from Texas Tech University, Lubbock, Texas, USA in 1988. He obtained his Master Degree in Electronics, Institute of Engineering Cybernetics, Wroclaw University of Science and Technology, Wroclaw, Poland in 1978. He also holds an International Business Certificate (Podyplomowe Studium Handlu Zagranicznego) from Warsaw School of Economics. His research interests are in control & system theory, information science and technology, manufacturing processes and pedagogy. He has over 50 refereed publications in various journals and international conference proceedings.

POLECAMY

HEAd'18

4th International Conference on Higher Education Advances (HEAd'18)
June 20 – 22, 2018 - Valencia (Spain)

After the great success of the third HEAd conference, which received submissions from 51 countries, we are pleased to announce the Fourth International Conference on Higher Education Advances (HEAd'18). This conference is an excellent forum for researchers and practitioners to exchange ideas, experiences, opinions and research results relating to the preparation of students, teaching/learning methodologies and the organization of educational systems.

Important dates

Submission deadline
February 9, 2018

Acceptance notification
April 11, 2018

Camera ready due
April 30, 2018

Conference
June 20-22, 2018

**4th International Conference on Higher Education Advances (HEAd'18),
20–22 czerwca 2018,
Valencia, Hiszpania**

Konferencja będzie forum wymiany pomysłów, doświadczeń, opinii i wyników badań związanych z przygotowaniem uczniów, metodami nauczania/uczenia się oraz organizowaniem systemów edukacyjnych.

Zagadnienia, które zostaną poruszone podczas wydarzenia, to m.in.:

- innowacyjne materiały i nowe narzędzia do nauczania
- doświadczenia w nauczaniu i uczeniu się
- technologia edukacyjna (wirtualne laboratoria, e-learning)
- nowe technologie w uczeniu się (np. MOOC, OER, grywalizacja)
- strategie edukacyjne
- doświadczenia poza klasą (praktyki, mobilność)
- nowe teorie i modele nauczania/uczenia się
- globalizacja edukacji
- akredytacja, jakość i ocena edukacji.

Więcej informacji można znaleźć na stronie: **http://www.headconf.org/**