Issues in Information Systems
Volume 18, Issue 3, pp. 170-183, 2017

ONE UNIVERSITY'S APPROACH TO DEVELOPING A CYBERSECURITY DEGREE AND EARN NSA CAE-CD CERTIFICATION

Gayle R. Jesse, West Liberty University, gayle.jesse@westliberty.edu

ABSTRACT

The purpose of this paper is to offer an example for higher education institutions seeking National Security Agency (NSA) certification for a cybersecurity degree program. A background in computer science (CS), information systems (IS), and information technology (IT) frames the project and supports the growth of cybersecurity degree programs and industry hiring trends. Furthermore, the paper explores four possible security degree options and correlating course sequencing at the undergraduate level. The NSA's National Centers of Academic Excellence in Cyber Defense (CAE-CD) mapping requirements are discussed for schools seeking certification. Finally, an approach is shared to guide schools working to meet NSA CAE-CD certification requirements.

Keywords: Cybersecurity, Information Assurance, Data Networking and Security, Information Security, NSA CAE-CD Program, Curriculum

INTRODUCTION

Information systems (IS) security is one of the hottest topics of conversation for information technology (IT) and computer science engineering professionals. Wallace (2015) states, "with countless threats and limited budgets, organizations can't eliminate all risks and must make careful assessments to manage them." Therefore, higher education institutions must respond and offer degree programs to meet newfound demands. Yet, with myriad higher education options available, how does a college distinguish itself from other institutions? Arguably, the best answer is for a school to build credibility and to establish a strong programmatic reputation by earning certifications and accreditations. The National Security Agency's (NSA) Center of Academic Excellence grants the most recognizable and rigorous certification for a security degree program.

The Internet produces countless opportunities for data access and information sharing. Unprecedented information access has allowed millions of people to connect in global ways, yet has created significant risks. Technology must be developed and utilized to protect the private information. Privacy technology and controls have manifested in numerous forms including: software and hardware encryption, read/write permission rights, and end-user multi-factor authentication protocols and procedures. The background section of this paper will discuss a legal precedent for data privacy, current cybersecurity threats, cybersecurity technologies and implementations presently available, and potential cybersecurity threats as examples of cybersecurity and emerging technology in the Information Age. The purpose of this paper is to provide a model for higher education institutions with a security degree program seeking NSA accreditation.

BACKGROUND

History

Since its inception in the 1960s, the Internet has grown from a basic network of interconnected computers to a vast and complicated information structure used by individuals, businesses, and governments. The potential uses for the Internet are nearly limitless; however, such immense capabilities can also cause profoundly dangerous situations. Therefore, private information must be protected from individuals and groups whose goal is to illegally obtain and use the information maliciously. All sensitive data should be protected from unauthorized access. This need for protection created the cybersecurity and information security fields and a demand for trained security professionals.

As sensitive information becomes increasingly available on the Internet, security technology must simultaneously improve and adapt. Moreover, the safeguarding technology must be readily available to businesses and individuals. Different cybersecurity strategies must be employed to counteract the growing risks of data breaches and hacks. Cybersecurity technology is constantly transforming. The creation of active and passive protection safeguards within software design, policy implementation, sound encryption algorithms, and practical training and usage demand ongoing scrutiny. While cybersecurity measures have existed for decades, cybersecurity is considered an ongoing process due to the continually changing nature, tactics, and technologies of the cyberthreats.

Solid cybersecurity cannot be overlooked. Data privacy remains a paramount concern for technology users; consequently, the need for data protection is, too. Cybersecurity experts and technology companies are continually challenged to adapt and update their knowledge, skills, and technologies to best combat threats and maintain effective data security. Successful cybersecurity requires a keen understanding of the need for privacy. Furthermore, cybersecurity threats, solutions, and future trends must emphasize effective information security. Undoubtedly, the demand for individuals with cybersecurity education and expertise will continue to grow.

DATA PRIVACY

Privacy is highly protected in the United States. The Fourth Amendment of the United State Constitution states, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (U.S. Const. Amend. IV)." While the Fourth Amendment was designed to protect citizens' private property from unwarranted governmental search and seizure, it has been applied to personal information, though in limited forms (Plotkin, 2012). As gleaned from United States Supreme Court cases, the right to privacy now includes personal information "that is disclosed to the government or is made available to corporations, and other private entities" (Plotkin, 2012, p. 4). Thus, individuals have the right to protect and maintain their privacy from others unless ordered by a judge-issued warrant. Americans also expect the federal government to keep them secure from harm (Westerhof, 2015). Another viewpoint emerges from companies who prefer to safeguard privacy and maintain cybersecurity, rather than enable the government's ability to bypass encryption or other cybersecurity protocols. Consequently, there must be a careful balance between the right to privacy and effective national security.

CYBERSECURITY THREATS

Cybercriminals use numerous methods to steal data or execute a cybersecurity threat. Easttom (2011) categorizes the six most common threats or attacks as: malware programs, security breaches, denial-of-service attacks, web attacks, session hijacking, and DNS poisoning. Each category, addressed below, possesses its own malfeasance.

Malware

Malware is defined as "a generic term or software that has a malicious purpose. It includes virus attacks, worms, adware, Trojan horses, and spyware" (Easttom, 2013). These malicious software programs are designed to gain control of a computer system by either inserting code into the system files or to send critical personal or system information to another computer. Other malware programs categorized as ransomware, like the infamous Crypto-locker, demand ransom from victims. Cybercriminals employ malware programs to glean information and/or harvest passwords from victims to gain financial or informational advantage (Elisan, 2012). Additionally, malware programs can be used to create bot-networks deployed in distributed denial-of-service (DDoS) attacks.

Security Breaches

Security breaches are designed to gain unauthorized access to a computer system via password cracking or other hacking means of elevated system privileges (Easttom, 2012). Recent security breaches include the Target, Inc., payment system breach and the United States Office of Personnel Management (OPM) data breach. During the Target breach, hackers accessed numerous locations' credit card payment terminals using the HVAC maintenance system. Target had a corporate agreement with a HVAC business to monitor several locations' climate control and the HVAC business' software had a weak common password. Hackers easily cracked the HVAC system password and stole Target customers' private debit and credit card information. The OPM security breach involved an elaborate phishing attack, combined with an Adobe Flash vulnerability, in a computer system. This attack allowed foreign hackers to access an OPM management official's login information, which opened the floodgates to sensitive federal employee data. However, these particular data breaches could have easily been avoided.

Denial-of-Service Attacks

A denial-of-service (DoS) attack is used to "deny the use of resources to legitimate users of the system, information, or capabilities" (Maiwald, 2013, p. 29). Essentially, a DoS or a distributed denial-of-service (DDoS) attack targets a subsystem(s) of servers or computers that controls a website's Internet connections (Singer & Friedman, 2014, p. 44). DoS/DDoS attacks prevent outgoing or incoming communication from a website or server. A DoS attack can generate catastrophic effects and the source can be difficult to track. Cybercriminals will often use tactics like botnets and other compromised computer systems to support DoS and DDoS attacks.

Web Attacks

Web attacks frequently occur because "any part of a website that allows for user interaction is also a potential point for attempting a web-based attack" (Easttom, 2013). Most data websites are built using the Simple Query Language (SQL) protocol, and hackers can easily attack using SQL injections. A hacker would simply enter specific commands into the username and password sections of a webpage login screen. The website database would read the commands and return information back to the attacker, thus granting access to the security settings and permitting the hacker to control the website (Singer & Friedman, 2014, p. 42).

Session Hijacking

Session hijacking is defined as an incident where an "attacker monitors an authenticated session between the client machine and the server and takes that session over" (Easttom, 2013). Session hijacking occur less frequently than other server or webpage attacks. Similarly, man-in-the-middle attacks allow the attacker to monitor data transfers by re-routing the transfers through a different server or computer system. The attacker seizes control over the data communications and possibly the entire communication session between the client and the server. Finally, another attack worth mentioning is domain name server (DNS) poisoning in which the attack spoofs the authenticated Internet Protocol (IP) address and captures private data for public distribution.

CYBERSECURITY METHODS

Cybersecurity strategies change frequently. Previously, cybersecurity prevention methods have followed *either* software- or hardware-based security protocols. However, security experts now recommend an integrated approach using *both* software and hardware security methods. Maiwald (2013) states, "if properly implemented and configured, it [the integrated approach] can reduce an organization's exposure to malicious programs."

Software-based Methods

Myriad software options exist to counteract cybersecurity threats. Anti-virus software will not prevent a computer system from downloading dangerous malware. However, "if properly implemented and configured, it [the anti-virus software] can reduce an organization's exposure to malicious programs" (Maiwald, 2013, p. 13). Another protective software is anti-spam software. Most Internet Service Providers (ISPs) and email providers include some form of anti-spam software. ISP anti-spam software typically includes antivirus, anti-spyware, anti-phishing, parental controls, software firewall, and identity theft protection (Alexander, 2009, p. 81). The anti-virus and anti-spam tools require monitoring and updates. An additional protective technique is sandboxing. Sandboxing is a software concept that isolates a software program, download, or attachment from the operating system (OS), so that it cannot affect the OS

(Easttom, 2013). One sandboxing example is Apple's iOS. All apps found on Apple mobile devices are isolated in a sandbox. Thus, the isolated apps are unable to directly affect the operating system without explicit user permission. Another cybersecurity strategy requires an end-user to provide additional information before gaining access (Rogers, Sharp, & Preece, 2011). One example is second-factor authentication. Second-factor authentication requires a user to log into a website or application and then enter a second temporary passcode to gain full access.

Hardware-based Methods

Hardware-based cybersecurity devices are another protection strategy. Physical devices are specifically designed to lock down a computer system, network, or physical area to only authorized personnel and/or to prevent data, personnel, or traffic from passing through a restricted zone or system. Examples of these hardware-based systems include: access cards, biometric devices, intrusion detection systems, and hardware-based firewalls.

Access cards

Access cards offer portable security verification because they can provide a second-factor authentication when combined with a personal identification number or password. Access cards are often used to enter restricted areas of a building or complex. Access cards normally exist in one of two forms: magnetic stripe (magstripe) or RFID (Radio Frequency Identification, also known as proximity cards) (McClure et al, 2012, p. 500). Businesses, government agencies, and other organizations regularly use integrate cards to authenticate security access, file permissions, and identity verifications in security policies.

Biometric devices

Biometric devices are among the most intriguing and recent security implementations. The devices are designed to read a biometric component unique to an individual person. Biometrics can read fingerprints, eye retinas, palm prints, facial recognition, or voice phrase recognition (Maiwald, 2013, p. 15). Apple, Inc, has been a biometric leader since integrating the TouchID fingerprint reader into the iPhone. Apple's use of biometrics has forced the entire mobile electronics industry to integrate biometrics as a primary form of device security. Increasingly, technology companies are implementing hardware-based biometric systems because they offer a higher level of security and are less prone to online hacking and malware attacks. Often, these systems are designed to work in conjunction with software encryption to provide an added layer of security. These systems are ideal for mobile devices like smartphones, tablets, and laptop computers because they provide enhanced information security with a superior end-user interface that appeals to consumers.

Hardware-based Firewalls

On the software side, Intrusion detection systems (IDS) are designed to provide system-wide monitoring of network and system activity. If the IDS discover irregular activity outside the preset parameters, the IDS automatically locks down the system and prevents unauthorized access or activity. However, a hardware-based firewall is designed as a sealed network-connected device containing an embedded operating system to prevent network traffic or software programs from modifying the internal network's settings, computers, or data (Schultz, 2000). Hardware-based firewalls resemble a honeypot because the firewalls filter network activity in an isolated area before external communication can reach the internal network devices. Hardware-based firewalls are intended to prevent end-users and hackers from accessing any portion of the firewall settings, essentially "eliminating the chance of a user-induced failure in the OS" (Schultz, 2000, p. 27).

CYBERSECURITY DEGREES AND CERTIFICATIONS

Hiring Trends

The Bureau of Labor Statistics Occupational Outlook Handbook (2015) indicated an 18% employment growth through 2024 for Information Security Analysts. This growth is significantly higher than all other occupations. Moreover, Modis (2017), an IT and engineering staffing firm, designated cybersecurity as a "hot" industry for job growth. Modis

(2017) divided cybersecurity jobs into six career areas with anticipated job growth through 2024: Analysis (21%), IT Security (18%), Managed Services and Project Management (15%), Health IT (15%), Web Development (27%), and Database Administration (11%).

Degree Growth

The Bureau of Labor Statistics reported over 200,000 unfulfilled cybersecurity jobs in 2015. Clearly, the demand for trained cybersecurity professionals outweighs the current supply. This demand further suggests that a lack of trained cybersecurity professionals increases the threat of cybersecurity attacks. Thus, educational institutions are developing undergraduate and graduate cybersecurity degree programs. However, the progress appears slow. There are two main reasons academia tends to lag behind industry when creating new degree programs: paperwork and faculty. First, a vast amount of paperwork must be completed and reviewed to create new degree programs. Each academic institution has its own requirements for creating new degrees, and the process must comply with accrediting bodies. Second, each school must have qualified faculty to teach the new course offerings. The faculty credentials must meet requirements established by the college and accrediting bodies. Finding qualified cybersecurity faculty is currently a bigger challenge than creating the cybersecurity degree programs.

Cybersecurity Certifications

Another challenge to the cybersecurity field is the need to complete industry certifications. Individuals seeking cybersecurity employment must have earned a college degree and also complete specific certifications. Entry-level certifications include: Security+, GSEC, CIPP, and SSCP. Advanced certifications include: CISSP, CISA, CISM, GCIH, and GCIA. However, approximately three-to-five years of work experience is required before taking advanced exams. Burning Glass (2015) stated that cybersecurity jobs are highly certificated with one in three (35%) positions requesting at least one certification, and CISSP is the most highly sought certification.

CURRICULUM REVIEW

About Liberty University

Liberty University (LU) is located in Lynchburg, Virginia. Founded in 1971, Liberty University currently has over 522 degree programs and the combined enrollment of residential and online students exceeds 110,000 (LU Quick Facts, 2016). The security degree programs are completed within the School of Engineering and Computational Sciences (SECS) and the School of Business (SoB). SECS is accredited by the Accreditation Board for Engineering and Technology (ABET) for both the Computing Accreditation Commission and Engineering Accreditation Commission. SoB is accredited by the Accreditation Council for Business Schools and Programs (ACBSP).

School of Engineering and Computational Sciences (SECS)

The School of Engineering and Computational Sciences (SECS) offers the Computer Science (CS) major. CS students are equipped with a firm foundation in algorithms and problem-solving. With a strong background in mathematics, students are able to utilize reason to analyze problems and then design, create, implement, and test software solutions.

SECS Program Learning Outcomes

Since SECS is ABET accredited, the Computer Science and Engineering programs are considered strong in applied science, computing, engineering, and engineering technology. ABET accreditation demonstrates that the program(s) are committed to providing students with a quality education, as encapsulated by five rigorous program learning outcomes (Liberty University, “SECS Catalog,” 2017).

School of Business (SoB)

Liberty University (Liberty University, "SoB Catalog," 2017) states that the School of Business (SoB) emphasizes building Champions for Christ, as well as strong businessmen and -women. This paper will only explore the Information Systems (IS) Assurance and Information Technology (IT) Data Networking and Security degrees. The IS Information Assurance program provides a solid academic foundation for students learning to manage operations critical to ensuring the integrity of an organization's informational assets, as well as identify and neutralize threats to sensitive data. The IT Data Networking and Security program equips students with critical knowledge in the field of networks and data security.

SoB IS and IT Program Learning Outcomes

The Accreditation Council for Business Schools and Programs (ACBSP) accredits the SoB at Liberty University. Both the IS and IT degree programs prepare students to meet the growing demand for information assurance professionals and data network and security administrators discussed in this paper. The IS and IT IS program learning outcomes can be found in the Liberty University "SoB Catalog" (2017).

Degree Options – Cognates (undergraduate)

Liberty University's Online Programs of Study (2016) define concentrations and cognates within majors based on a required number of completed credit hours. Concentrations require 18+ completed credit hours; cognates require 9-17 completed credit hours. The SoB, with the School of Engineering, offers four security degree options. SECS offers two security cognates: Cybersecurity and Information Security. SoB also offers two security-based cognates: a Business Management Information Systems (BMIS) degree with a cognate in Information Assurance and a Business Management Information Technology (BMIT) degree with a cognate in Data Networking and Security.

Cognate Degree Requirements

This section of the paper discusses Liberty University's degree requirements for the four security cognates. Currently, each of the security degree programs at Liberty University continues to grow. LU's Computer Science Cybersecurity Degree Completion Plans (DCPs), along with Suggested Course Sequencing, can be viewed in the appendix. URLs for all are four degrees are provided in the reference section.

Information Systems (IS) Information Assurance Cognate courses include: Networks, Network Security, Information Security Planning, Cybersecurity, and Digital Forensics (SoB, IS IA, 2017). IT Data Networking and Security Cognate courses include: Networks, Network Security, Cybersecurity, Information Security Planning, and Advanced Networking and Communication Systems (SoB, IT DNS, 2017). CS Information Security Cognate courses include: Studies in Information Security, Information Security Planning, Information Security Operations, and Technical Aspects of Computer Security or Modern Cryptograph (SECS, CS IS, 2017). CS Cybersecurity Cognate courses include: Studies in Information Security, Introduction to Linux, Technical Aspects of Computer Security, and Modern Cryptography (SECS, CS, 2017).

Finally, if students are interested in pursuing a minor, Liberty offers a CS Information Security Minor consisting of 18 credits or six courses. Courses to complete the minor include: Principles of Management, Business Data Communication Systems, Studies in Information Security, Information Security Planning, Information Security Operations, and the choice of either Intro. to Homeland Security or Intro. to Intelligence and National Security.

NSA CAE-CD CERTIFICATION

About NSA CAE-CD Certification

The National Centers of Academic Excellence in Cyber Defense's website explains the NSA CAE-CD Certification. "The National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National

Centers of Academic Excellence in Cyber Defense (CAE-CD) program. The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise for the Nation. CAE-CD institutions receive formal recognition from the U.S. Government as well as opportunities for prestige and publicity for their role in securing our Nation's information systems. Designation as a Center does not carry a commitment of funding from NSA or DHS; however, funding opportunities may become available periodically (e.g., NSF). An additional program that complements this certification is the CAE-Cyber Operations program. Cyber Operations focuses on technologies and techniques related to specialized cyber operations (e.g., collection, exploitation, and response) to enhance the national security posture of our Nation. The CAE-Cyber Operations program supports the President's National Initiative for Cybersecurity Education (NICE): Building a Digital Nation and furthers the goal to broaden the pool of skilled workers capable of supporting a cyber-secure nation (NSA CAE-CD, 2016)."

Certification Requirements

The CAE-CD program encompasses the following designations: Four-Year Baccalaureate/Graduate Education (CAE-CDE), Two-Year Education (CAE2Y) and Research (CAE-R) (NSA CAE-CD, 2016). Prospective schools must ensure their programs meet stringent CAE criteria and mapping curricula that match a core set of cyber defense knowledge units (NSA CAE-CD, 2016). Schools may also elect to map their curricula to specialized Focus Areas, though Liberty University elected not to offer a specialized focus area. Liberty University plans to file for the CAE-CDE certification at the end of 2017; thus, the next section of this paper will only discuss the CAE-CDE certification process using standard mapping criteria. Designation as a National CAE-CDE lasts for five academic years and then the school must re-apply to retain designation. CAE-CDE requirements are divided into Knowledge Units (KUs) Mapping and Program Requirements.

Knowledge Units (KUs) Mappings

Knowledge Units (KUs) Mapping plans an institution's curricula to meet the six core Knowledge Units (KUs) over four years, plus five optional units (51 total options). Furthermore, schools must provide evidence that a student can reasonably complete the program to meet all identified KUs. The six main KUs are: Database Management Systems, Network Defense, Network Technology and Protocols, Operating Systems Concepts, Probability and Statistics, and Programming. Each KU outlines the topics and outcomes each student must complete. Each school must select the five optional KUs, and while topics and outcomes are provided, students must demonstrate mastery. An Excel spreadsheet contains the mapping matrix with all KUs and can be found online: https://www.iad.gov/NIETP/CAERequirements.cfm (NSA CAE-CD MAPPINGS, 2017). An example of Database Management Systems topics and outcomes is provided in the appendix.

Program Criteria

Program requirements must address the following eight areas: Cyber Defense Academic Program Path, "Center" for CD Education, Student-based Cyber Defense Skills Development, Cyber Defense Faculty and Courses Taught, Cyber Defense Faculty Expertise and Research, Cyber Defense is a Multidisciplinary Practice at the Institution, Institution Information System (IS) Security, Cyber Defense Outreach Beyond the Institution.

Initially, schools must submit a "**Letter of Endorsement and Intent,**" which provides official notice of institutional endorsement and intent to participate in the CAE-CDE program. The eight actual program areas are as follows and have been condensed to fit within the paper constraints. A full version can be found online: https://www.iad.gov/NIETP/documents/Requirements/CAE_CDE_criteria.pdf (CAE-CD Criteria, 2017).

1. **Cyber Defense Academic Program Path**. The Cyber Defense (CD) Program Path must have existed for at least three (3) years.
2. **"Center" for CD Education**. The institution must have an officially established entity (either physical or virtual) serving as the focal point for its CD educational program. The center shall provide specified service and be supported by a website.

3. **Student-based Cyber Defense Skills Development**. The institution must explain how it fosters student development in the field of Cyber Defense, as well as the contributions to CD evolution of theory and practice in the field. This is met by relating the developed student skills back to one or more of the mapped KUs.
4. **Cyber Defense Faculty and Courses Taught**. The institution must demonstrate that it has sufficient faculty members, either full- or part-time, who are responsible for the overall CD program of study and to ensure program continuity.
5. **Cyber Defense Faculty Expertise and Research**. The institution must show that faculty members are Cyber Defense experts and are active in current CD practice and research including: publications, presentations, and professional societies, as well as seeking grants for CD resources and mentoring CD students.
6. **Cyber Defense is a Multidisciplinary Practice at the Institution**. The institution must demonstrate that CD is not treated as a separate discipline, but is integrated into additional degree programs within the institution.
7. **Institution Information System (IS) Security**. The system security-planning objective is to improve the protection of information system resources.
8. **Cyber Defense Outreach Beyond the Institution**. The institution must express how Cyber Defense practices extend beyond normal institutional boundaries by sharing CD principles with others.

APPROACH TO MEETING THE NSA CAE-CD REQUIREMENTS

The ideal way to approach NSA CAE certification is to consider the certification process as a project. Schwalbe (2015) discuss Project Management Body of Knowledge (PMBOKs) five project management process groups: Initiating, Planning, Executing, Monitoring and Controlling, and Closing. Initiating the project involves gaining the support of the school administration and faculty/staff. Planning is critical when working to meet the rigorous CAE criteria and KUs mapping curricula. Schwalbe (2015) defines a project management plan as "a document that is used to coordinate all project planning documents and helps to guide a project's execution and control." Therefore, a clear plan must be created to meet the NSA CAE certification requirements. Furthermore, all faculty/staff involved in the certification process should be involved in creating the project management plan. Faculty/staff involvement ensures transparency and clarity about the expectations of teach person's role. Once the plan is finalized, the execution process can begin, and faculty/staff can complete tasks generated in the planning phase. Performance is based on how well the project team executes the plan. Moreover, it is recommended that one individual, possibly the department chair or dean of the cyber defense program, will manage the certification process. The managing individual will complete the fourth phase, the monitoring and controlling phase. Monitoring and controlling lasts for the duration of a project, and the person monitoring and controlling must meet regularly with the faculty/staff involved to determine if tasks are being completed according to the plan. Finally, the person managing the project will complete the final project phase. The manager will ensure that all project components have been fully completed and loaded into the submission site properly before submitting the required materials.

The NSA/DHS provides an Excel spreadsheet titled "CAE KU Mapping Matrix." The matrix's purpose is to map curricula to match the Knowledge Units (KUS). The NSA/DHS recommends that institutions begin the mapping process by adding the school's course numbers within the corresponding KUs. Since multiple professors may teach the same course across sections and/or semesters, one professor should be assigned a specific course(s) and then collect information across sections. Each course instructor will complete the KUs by inserting a topic/objective/week/session/etc. number that relates to their courses. Once instructors have completed all course submissions, the professor tasked with generating the final mappings should merge all documents into one master KU document used to enter information into the CAE application website.

The following approach is recommended to complete the eight program criteria. Each area is worth a specific number of points; an area is considered complete after meeting a minimum value. The author of this paper completed area eight. An Excel spreadsheet was created to complete this NSA CAE requirement. The spreadsheet listed the requirements of each section and detailed entries explained how the requirements were fulfilled. The author suggests that at least one item in each section be thoroughly completed. An image of this spreadsheet is offered in the appendix.

CONCLUSION

Cybersecurity Importance

Cyberattacks are rampant. In recent years, the U.S. government invited a number of journalists to the Idaho National Laboratory to display the dangers and threats of a cyberattack (Singer & Friedman, 2014). Additionally, government officials wanted to display critical nature of the situation and to make the journalists and public understand that not even the U.S. government could stop an all-out cyberattack (Singer & Friedman, 2014). In the examples highlighted by the Target and OPM security breaches, the lack of effective cybersecurity protocols and awareness cost both Target and the federal government millions of dollars. The OPM case was particularly dangerous because a significant threat to national security also leaves federal employees susceptible to foreign attack and influence. Cybersecurity attacks could potentially collapse the financial and civic institutions within society

Cybersecurity Future Threats & Trends

Cybersecurity threats are changing swiftly. Cybercriminals use rootkits and bots more frequently to accomplish their malicious objectives. Rootkits are hard to detect. These rootkits are projected to adapt and evolve with the growing usage of mobile devices and new operating systems (Eilsan, 2012). Cybercriminals have also utilized botnets. Experts are concerned that botnets will concentrate on social media networks as a command and control medium (Eilsan, 2012). Botnets could easily monitor a social media website for impending traffic regarding the upcoming release of new smartphone, and then release a massive phishing attack through other spam botnets, prompting people to click on a spam message hyperlink that could engage a ransomware program (Eilsan, 2012).

The research and recommendations presented in this paper clearly ground the need for solid cybersecurity education and strategies. Moreover, the general public is growing ever more aware of the need for cybersecurity measures. Even though cybersecurity software, hardware, and policies have been around for the last few decades, cybersecurity is still considered an emerging technology based on the continually changing nature, tactics, and technologies presented by the cyberthreats. Data privacy and protection will remain paramount for all technology users. Cybersecurity experts and technology companies will be constantly challenged to combat threats and maintain security. Cybersecurity will only be successful if educated professionals understand the need for privacy, the types of cybersecurity threats, the available cybersecurity solutions, and critical importance of maintaining effective information security. Georgescu and Tudor (2015) further warn that cyber terrorism's "…objectives are: taking control of networks that regulate critical infrastructure such as water supply networks, air traffic, the energy, military networks, traffic signs system, financial systems, telecommunications etc.; taking control of industrial systems and energy; theft technology, business plans, projects and insider trading information or secrets" (p. 115). Without cybersecurity technologies and professionals, cyberthreats have the potential to cripple society.

Final Insights

In closing, this paper offered recommendations and an example for higher education schools seeking NSA certification for a cybersecurity degree program. A literature review grounded an understanding of cybersecurity, cybersecurity degree program growth, and industry hiring trends. If a school wants to develop a cybersecurity degree program, this paper provided four options and course sequencing, which gives students a plan to follow for degree completion. Additionally, NSA CAE-CD mapping requirements were discussed and one university's approach to the certification process was described to help other schools aligning their security degree program to meet NSA CAE requirements.

The most important element of this paper centers on information security. Wallace (2015) states that information is an asset that needs protection, and organizations are legally required to safely secure medical records, financial information, social security numbers, academic records, and other sensitive data such as government classified documents. Current research and industry trends suggest technology-based employment will grow by 12% versus 6.5% in all other industries by 2024 (Modis 2017). Additional forecasts indicate potential for 488,500 new tech jobs by 2024. Students must understand that self-study and certification completion beyond the general degree program requirements are essential for the competitive job market. Finally, while this paper provides one plan to secure NSA CAE certification, each institution must adopt a process that meets its own unique needs.

REFERENCES

Alexander, P. (2009) *Home and Small Business Guide to Protecting Your Computer Network, Electronic Assets, and Privacy.* Praeger Publishers, Westport, CT: Greenwood Publishing Group.

Bureau of Labor Statistics. (2015). U.S. Department of Labor, Occupational Outlook Handbook, 2016-17 Edition, Information Security Analysts. Retrieved March 27, 2017, from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

Burning Glass. (2015). Cybersecurity Jobs Report. Retrieved March 29, 2017, from http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf.

CAE-CD Criteria. (2017). *National Centers of Academic Excellence in Cyber Defense (CAE-CDE) Education Program Criteria for Measurement* [PDF]. Meade: National Centers of Academic Excellence in Cyber Defense. https://www.iad.gov/NIETP/documents/Requirements/CAE_CDE_criteria.pdf

Easttom, W. (2011) *Computer Security Fundamentals, 2nd Edition.* Indianapolis, IN: Pearson, Inc. Retrieved from http://techbus.safaribooksonline.com/book/networking/security/9780132828284.

Elisan, C. C. (2012). *Malware, Rootkits & Botnets: A Beginners Guide.* United States: McGraw-Hill Osborne Media.

Georgescu, C., & Tudor, M. (2015). Cyber Terrorism Threats To Critical Infrastructures Nato's Role In Cyber Defense. Knowledge Horizons. Economics, 7(2), 115-118. Retrieved from http://ezproxy.liberty.edu:2048/login?url=http://search.proquest.com/docview/1686096993?accountid=12085.

Liberty University Online Programs of Study. (2016). Retrieved January 27, 2016, from http://www.liberty.edu/academics/catalogs/?PID=25706.

Liberty University Quick Facts. (2016). Retrieved January 27, 2016, from https://www.liberty.edu/aboutliberty/?PID=6925.

Liberty University, SECS. (2017). School of Business, Undergraduate Catalog 2016-2017. Retrieved May 06, 2017, from https://www.liberty.edu/index.cfm?PID=33765

Liberty University, SoB. (2017). School of Engineering & Computational Sciences, Undergraduate Catalog 2016-2017. Retrieved May 06, 2017, from https://www.liberty.edu/index.cfm?PID=33774Maiwald, E. (2013). *Network Security: A Beginner's Guide, 2nd Edition*. New York: McGraw-Hill.

McClure, S., Scambray, J., Kurtz, G. (2012). *Hacking Exposed 7: Network Security Secrets & Solutions.* New York: McGraw-Hill.

Modis. (2017). Tech Jobs On The Rise: Tops in Tech - The 18 Most In-Demand IT Jobs In 2017. Retrieved March 29, 2017, from http://www.modis.com/it-insights/infographics/top-it-jobs-of-2017/.

NSA CAE-CD. (2016, May 03). National Centers of Academic Excellence in Cyber Defense. Retrieved May 07, 2017, from https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/

NSA CAE-CD MAPPINGS. (2017). CAE Requirements and Resources. Retrieved May 7, 2017, from https://www.iad.gov/NIETP/CAERequirements.cfm

Plotkin, R. (2012). *Privacy, Security, and Cyberspace.* New York: Checkmark Books.
Schwalbe, K. (2015). *Information technology project management*. United States: Cengage Learning.

Schultz, K. (2000, February 21). Firewall Appliances -- Keep The Barbarians away -- Hardware-Based Firewall Appliances Come With Virtual Private Networking Support. InternetWeek, 27. Retrieved from http://ezproxy.liberty.edu:2048/login?url=http://go.galegroup.com.ezproxy.liberty.edu:2048/ps/i.do?id=GALE%7CA59561030&sid=summon&v=2.1&u=vic_liberty&it=r&p=GRGM&sw=w&asid=43d8938adc162b93d92056f910d54cba.

SECS, CS IS. (2017, March 31). Bachelor of Science in Computer Science Information Security Cognate 2017-2018 Degree Completion Plan [PDF]. Lynchburg: Liberty University. http://www.liberty.edu/media/1270/CSIS-BS-R.pdf

SECS, CS. (2017, March 31). Bachelor of Science in Computer Science Cyber Security Cognate 2017-2018 Degree Completion Plan [PDF]. Lynchburg: Liberty University. http://www.liberty.edu/media/1270/CSCS-BS-R.pdf

Singer, P.W., Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York: Oxford University Press.

SoB, IS IA. (2017, March 31). Bachelor of Science in Information Systems Information Assurance Cognate 2017-2018 Degree Completion Plan [PDF]. Lynchburg: Liberty University. http://www.liberty.edu/media/1270/ISIA-BS-R.pdf

SoB, IT DNS. (2017, March 31). Bachelor of Science in Information Technology Data Networking and Security Cognate 2017-2018 Degree Completion Plan [PDF]. Lynchburg: Liberty University. http://www.liberty.edu/media/1270/ITDS-BS-R.pdf

Rodgers, Y., Sharp, H., & Preece, J. (2011). *Interaction Design: Beyond Human-Computer Interaction* (3rd ed.). Retrieved from http://www.safaribooksonline.com/.

United States Constitution: Amendment IV. (1789).

Wallace, P. M. (2015). *Introduction to information systems.* Boston: Pearson.

Westerhof, C. (2015). *Annual Editions: Technologies, Social Media, and Society*, 21/E. United States: McGraw Hill Higher Education.

APPENDIX A

KU Mapping Example of Database Management Systems Topics and Outcomes

3	**Database Management Systems**
4	The intent of this Knowledge Unit is to provide students with the skills to utilize
5	**Topics**
6	Overview of database types (e.g., flat, relational, network, object-oriented)
7	SQL (for queries)
8	Advanced SQL (for DBMS administration – e.g., user creation/deletion, permissions and access controls)
9	Indexing, Inference, Aggregation, Polyinstantiation
10	How to protect data (confidentiality, integrity and availability in a DBMS context)
11	Vulnerabilities (e.g., SQL injection)
12	**Outcomes**
13	Students will be able to:
14	List the most common structures for storing data in a database management system
15	Configure a commodity DBMS for secure access
16	Describe alternatives to relational DBMSs and their unique security issues
17	Describe the role of a database, a DBMS, and a database server within a complex system supporting multiple applications
18	Demonstrate basic SQL proficiency for table creation, data insertion and data query
19	Describe DBMS access controls and privilege levels and apply them to a simple database
20	Develop a DB structure for a specific system/problem.

Approach to completing Criteria Areas (#8)

	A	B–G	H–N
1	**Liberty University -- NSA CAE-CD -- Outreach Beyond the Institution**		
2	**A. Shared Curriculum or Advancing Cyber Defense Educational Practice**		˚Provide evidence of how the institution shares it CD curriculum and/or faculty with
3	1		other schools, to include K-12 schools, community colleges, technical schools, minority
4	2		colleges/universities to advance cyber defense knowledge within the last 3 years
5	3		˚Provide specific information about sponsorship or participation in CD curriculum
6	4		development workshops or colloquia or faculty sharing events for any of the types listed
7	5		above within the last 3 years
8	**B. Tranfer Credit**		˚Provide evidence that the institution awards credit in CD courses and/or technical
9	1		prerequisite courses from other academic institutions or through alternative means.
10	2		Examples include, (but are not limited to): statewide transfer agreements, articulation
11	3		agreements, college in the high school, dual credit, running start, credit for prior
12	4		learning, credit for military training or occupation
13	5		
14	**C. Community Outreach**		˚Provide evidence of faculty/employee sponsorship or oversight of CD events for the
15	1		community at large. Events could include CD awareness and education for local schools,
16	2		adult education centers, senior centers, camps, first responders and the surrounding
17	3		community
18	4		˚Examples of events could be, but are not limited to, computer "check-up" days,
19	5		protecting personal information in cyber space, workshops for senior citizens on
20			Internet safety, or preventing and recovering from a "virus"
21	**D. Sponsorship or Participation in CD exercises, Capture the Flag & other Cyber Related Competitions**		
22	1		˚Provide evidence of participation in or sponsorship of CD exercises and competitions
23	2		within the last 3 years, (e.g., link to team roster on the competition website, link to
24	3		social media about the exercise, etc.)
25	4		˚Explain the benefit of participating in the Cyber Defense Exercise/Competition. How did
26	5		the team place? What were the lessons learned? What basic cyber content was
27			reinforced by participating on a team?
28	**E. CAE Collaboration**		
29	1		˚Provide evidence on how the institutions partners with other CAE schools on research or
30	2		shared classes/events
31	3		˚Evidence can include collaboration on papers, grants, cyber camps, etc.
32	4		˚Provide evidence of performing reviews or acting as a mentor for the CAE CD program
33	5		˚Provide evidence of presenting a CAE Tech Talk for the CAE Community
34	**F. Cyber Defense Business/Industry Collaboration**		˚Provide evidence on how the institution partners with companies and other employers
35	1		to identify Cyber Defense needs of potential employers and encourage student
36	2		internships
37	3		˚Provide evidence on how the institution works with employers and students to support
38	4		placement for Cyber related jobs
39	5		˚Provide evidence of obtaining input on curriculum to meet industry needs

Cyber Security Degree Completion Plan

LIBERTY UNIVERSITY

Bachelor of Science in Computer Science
Cyber Security Cognate
2017-2018 Degree Completion Plan

Important: This degree plan is effective for those starting this degree program in fall 2017 through summer 2018. This degree plan will remain in effect for students who do not break enrollment or who do not change degree programs, concentrations or cognates.

GENERAL EDUCATION/
CORE COMPETENCY REQUIREMENTS (44-47 hours)

Course		Hrs	Sem	Grade
Communication (6 hours)[1]				
ENGL 101	Composition & Rhetoric	3	____	____
________	Communications Elective	3	____	____
Math, Science & Technology (7-10 hours)[1]				
MATH ____	Math Elective (MATH 114 or higher)	3	____	____
________	Natural Science Elective	3	____	____
________	Technology Competency[2]	0-3	____	____
UNIV 101	University Core Competencies	1	____	____
Information Literacy (7 hours)[1]				
INQR 101	Inquiry 101	1	____	____
________	Composition Elective	3	____	____
________	Information Literacy Elective	3	____	____
Critical Thinking (12 hours)[1]				
RSCH 201	Research 201	3	____	____
________	Literature OR Philosophy Elective	3	____	____
________	Social Science Elective	3	____	____
________	Cultural Studies Elective	3	____	____
Christian Life & Thought (12 hours)[1,3]				
BIBL 105	Old Testament Survey	2	____	____
BIBL 110	New Testament Survey	2	____	____
EVAN 101	Evangelism & Christian Life	2	____	____
RLGN 105	Intr Bwvw/Contemp Moral Issues	2	____	____
THEO 201	Theology Survey I	2	____	____
THEO 202	Theology Survey II	2	____	____

Course		Hrs	Sem	Grade
Major Foundational Courses (4-15 hours)[4]				
ENGR 270	Technical Communication	3	____	____
MATH 131	Calculus & Analytical Geometry I[5]	4	____	____
MATH 132	Calculus & Analytical Geometry II[5]	4	____	____
PHYS 231	University Physics I	4	____	____
MAJOR				
	Core (39 hours)			
CSIS 100	Intro. to Information Sciences & Systems	3	____	____
CSIS 110	Introduction to Computing Sciences	3	____	____
CSIS 111	Introduction to Programming	3	____	____
CSIS 112	Advanced Programming	3	____	____
CSIS 215	Algorithms & Data Structures	3	____	____
CSIS 326	Database System Concepts	3	____	____
CSIS 342	Computer Architecture & Organization	3	____	____
CSIS 355	Network Architecture & Protocols	3	____	____
CSIS 434	Theory of Programming Languages	3	____	____
CSIS 443	Operating Systems	3	____	____
CSIS 471	Software Engineering	3	____	____
CSIS 481	CS Capstone I	3	____	____
CSIS 482	CS Capstone II	3	____	____
	Cognate (12 hours)			
CSIS 340	Studies in Information Security	3	____	____
CSIS 345	Introduction to Linux	3	____	____
CSIS 461	Technical Aspects of Computer Security	3	____	____
CSIS 463	Modern Cryptography	3	____	____
Quantitative Studies Elective Courses (10 hours)				
ENGR 133	Calculus with MATLAB			
or MATH 133	Calculus with Mathematica Lab	1	____	____
MATH 211	Introduction to Statistical Analysis	3	____	____
MATH 250	Introduction to Discrete Mathematics	3	____	____
MATH 350	Discrete Mathematics	3	____	____
Lab Sciences Courses (8 hours)				
________	Natural Science Elective[6]	4	____	____
________	Lab Science Elective[7]	4	____	____
Technical Elective Courses (12-15 hours)[8]				
CRST 290	History of Life	2	____	____
________	________________	_	____	____
________	________________	_	____	____
________	________________	_	____	____

Cyber Security Degree Suggested Course Sequence

SUGGESTED COURSE SEQUENCE

FRESHMAN YEAR

First Semester		Second Semester	
ENGL 101	3	EVAN 101	2
MATH 131[1]	4	INQR 101	1
UNIV 101	1	RLGN 105	2
Technology Competency[2]	0-3	Communications Elective[3] [ENGR 270]	3
CSIS 100	3	Composition Elective[3]	3
CSIS 110	3	Math Elective[3] [MATH 132[1]]	4
MATH 133 or ENGR 133	1	CSIS 111	3
CSER	0	CSER	0
	Total 15-18		Total 18

SOPHOMORE YEAR

BIBL 105	2	BIBL 110	2
Natural Science Elective[3] [PHYS 231]	4	RSCH 201	3
Social Science Elective[3]	3	Literature/Philosophy Elective[3]	3
CRST 290	2-3	CSIS 215	3
CSIS 112	3	MATH 250	3
MATH 211	3	Lab Science Elective[4]	4
CSER	0	CSER	0
	Total 17-18		Total 18

JUNIOR YEAR

THEO 201	2	THEO 202	2
Natural Science Elective[5]	4	Cultural Studies Elective[3]	3
CSIS 326	3	CSIS 340	3
CSIS 342	3	CSIS 434	3
CSIS 355	3	CSIS 443	3
MATH 350	3	CSIS 471	3
CSER	0	CSER	0
	Total 18		Total 17

SENIOR YEAR

Information Literacy Elective[3]	3	CSIS 461	3
Social Science Elective[3]	3	CSIS 463	3
CSIS 345	3	CSIS 482	3
CSIS 481	3	Technical Elective[6]	3
Technical Elective[6]	3	Technical Elective[6]	3
Technical Elective[6]	3	CSER	0
CSER	0		Total 15
	Total 18		