Volume 13, No. 3
May 2015
ISSN: 1545-679X

INFORMATION SYSTEMS EDUCATION JOURNAL

In this issue:

The **Information Systems Education Journal** (ISEDJ) is a double-blind peer-reviewed academic journal published by **EDSIG**, the Education Special Interest Group of AITP, the Association of Information Technology Professionals (Chicago, Illinois). Publishing frequency is six times per year. The first year of publication is 2003.

ISEDJ is published online (http://isedjorg). Our sister publication, the Proceedings of EDSIG (http://www.edsigcon.org) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the ISEDJ journal. Currently the target acceptance rate for the journal is under 40%.

Information Systems Education Journal is pleased to be listed in the 1st Edition of Cabell's Directory of Publishing Opportunities in Educational Technology and Library Science, in both the electronic and printed editions. Questions should be addressed to the editor at editor@isedj.org or the publisher at publisher@isedj.org.

INFORMATION SYSTEMS EDUCATION JOURNAL

Cybersecurity Curriculum Development: Introducing Specialties in a Graduate Program

Ali Bicak
abicak@marymount.edu

Michelle (Xiang) Liu
xliu@marymount.edu

Diane Murphy
dmurphy@marymount.edu

Information Technology and Management Science Department
Marymount University
Arlington, Virginia 22207, USA

Abstract

The cybersecurity curriculum has grown dramatically over the past decade: once it was just a couple of courses in a computer science graduate program. Today cybersecurity is introduced at the high school level, incorporated into undergraduate computer science and information systems programs, and has resulted in a variety of cybersecurity-specific graduate programs. However, is that even enough? Is cybersecurity so broad that education needs to be more specialized? Employers want graduates who can hit the ground running: not in the broad field of cybersecurity but in some very specific areas**.**

This paper is structured as follows. First, we will provide a brief overview of the current approaches to cybersecurity education including government standards bodies such as the National Initiative for Cybersecurity Education (NICE) framework, the upcoming changes in the National Information Assurance (IA) Education and Training Programs (NIETP) Center of Academic Excellence (CAE) designation requirements, and the Department of Labor competency model. Second, we will present a framework for curriculum changes, which we use to determine the viability of information technology/information systems (IS/IT) curriculum changes to our departmental educational offerings. We examine relationships with other departments and how cybersecurity is enhanced by other domain knowledge. Then we discuss the three specialties we plan to introduce in the cybersecurity graduate curriculum: cybersecurity data analysis, cyber intelligence, and health care information security and privacy. Finally, the future cybersecurity curriculum directions are presented and discussed.

Keywords: cybersecurity, curriculum development, data analysis, cyber intelligence, health care, security and privacy.

1. BACKGROUND

Our university is a small, private four-year institution in the Washington, DC metropolitan area, close to many Federal government offices. We are accredited by the Commission on Colleges of the Southern Association of Colleges and Schools (SACS) to award degrees at the doctoral, master's and bachelor's levels. We currently offer both undergraduate and graduate programs in IT, with specialties in cybersecurity. These are largely face-to-face programs with a small online component. In addition, we introduced a 36-credit online cybersecurity program in the past two years.

The International Telecommunication Union (ITU) defines cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment." (ITU-T, 2014). Despite the emphasis on cyber environment, which makes cybersecurity a subset of the traditional field of "information security", both terms are used interchangeably today due to continuous discovery of security issues and increasing risk in cyberspace. Cybersecurity is a fast growing discipline with new fields and products, such as security incident and event management (SIEM), risk management frameworks, and industry-specific applications, appearing constantly.

As an academic institution, how do we ensure that our degree offerings stay current with workplace needs while ensuring our students have the fundamental knowledge necessary to meet the cybersecurity challenges of tomorrow?

2. EDUCATION VS. TRAINING VS. CERTIFICATION

There is no doubt that to master cybersecurity, professionals need both knowledge and experience as shown in Figure 1 below.

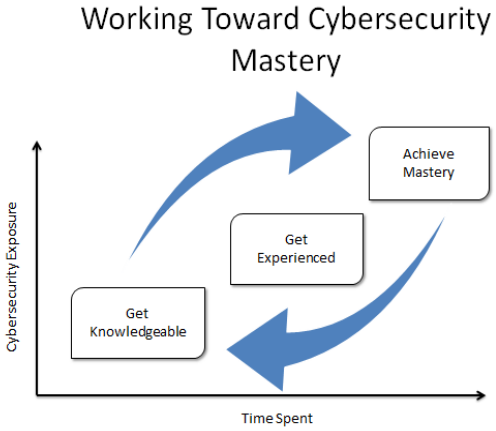

Figure 1: Mastering Cybersecurity knowledge and skills

Both training and education play a role in developing the necessary cybersecurity knowledge base (Woener, 2012). Education can be considered strategic and provides the foundation for the context for security concepts, tools, technologies, etc. and is acquired through formal studies over a period of time. Cybersecurity training may be considered tactical and puts emphasis on explicit skills; therefore, it is usually short term and may be directed to earning a specific certification.

There has been an increasing focus on training and certification in the cybersecurity field, at least, in part, due to the Defense Department Directive 8570, which requires military, civilian and contract personnel who handle cybersecurity for department systems to have certifications appropriate for the job they perform. First issued in 2005, the requirements have been updated three times to show changing requirements (Department of Defense, 2014).

In 2013, the U.S. Department of Homeland Security (DHS) launched the National Initiative for Cybersecurity Careers and Studies (NICCS), an online resource for cybersecurity career, education, and training information in the continuum from high school to graduate levels (niccs.us-cert.gov).

As educators, we must be strategically aware of the evolution of the fast changing cybersecurity discipline and provide programs that prepare our students for the cybersecurity environment of tomorrow, while being aware of the employment needs in the field, including training and certifications.

NICE

An important consideration is the National Initiative for Cybersecurity Education (NICE) framework (csrc.nist.gov/nice/framework/), developed by the National Institute for Standards and Technology (NIST). This organizes some 32 cybersecurity skills and knowledge units in seven categories, recognizing the need both for technical and managerial skills and for a comprehensive knowledge background in implementing a coherent cybersecurity program, as shown in Figure 2.

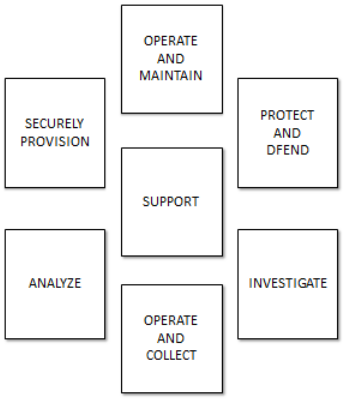

Figure 2. Seven Categories of NICE Framework (Adapted from csrc.nist.gov)

Each of these knowledge categories represents several specialties. For example, the "Operate and Collect" category includes "specialty areas responsible for the highly specialized and largely classified collection of cybersecurity information that may be used to develop "intelligence" leading to the idea of a cyber intelligence component to our program. In addition, the "investigate" category includes "specialty areas responsible for the investigation of cyber events or crimes which occur within IT Systems and networks." Threat reports show that health care is a primary target for cyber criminals and so becomes a consideration for a component of our program (Filkins, 2014). Finally the "analyze:" category includes "specialty areas responsible for highly specialized and largely classified review and evaluation of incoming cybersecurity information", leading to the idea of a cybersecurity data analysis component to our program.

Centers of Academic Excellence

The Colloquium for Information Systems Security Education (CISSE) is one of the leading proponents for cybersecurity education at the higher education level (www.cisse.info). In defining requirements for cybersecurity education, CISSE encourages university programs to receive the National Security Agency/Department of Homeland Security designation of National Center for Academic Excellence in Information Assurance Education (CAE/IAE) (Anderson, 2013). Until very recently, this designation required meeting the criteria defined by Committee on National Security Systems (CNSS). These were essentially the training requirements for specific cybersecurity positions in the defense and intelligence agencies such as the ISSO (Information Systems Security Officer) or systems administrator.

However, these standards are now changing as the National Information Assurance (IA) Education and Training Programs (NIETP) office, the organization that designates CAE/IAE. The designation has been renamed to the Information Assurance/Cyber Defense (IA/CD) and the criteria for designation have been extensively revised "to better reflect the state to which the discipline of IA has evolved since the original publication of the training standards" (www.iad.gov/NIETP). All existing institutions must apply for redesignation by December 2014. The revised NIETP requirements, well aligned with the NICE framework, use a system of knowledge units and focus areas that enable differentiation amongst the higher education institutions by allowing each school to recognize its specific focus areas of research and/or educational offerings. The new standards require programs at 4-year schools (including graduate programs) to cover all the seventeen required and five of the optional Knowledge Units (KUs) to become a CAE IA/CD institution. In addition, the CAE also provides the option for those schools to apply for one or more "Focus Area" designations for their programs. Those focus areas are listed in Figure 3.

Cyber Investigations
Data Management Systems Security
Data Security Analysis
Digital Forensics
Health Care Security
Industrial Control Systems-SCADA Security
Network Security Administration
Network Security Engineering
Secure Cloud Computing
Secure Embedded Systems
Secure Mobile Technology
Secure Software Development
Secure Telecommunications
Security Incident Analysis and Response
Security Policy Development and Compliance
Systems Security Administration
Systems Security Engineering

Figure 3. CAE IA/CD Focus Areas

These suggest that cybersecurity data analysis (listed here as data security analysis) and health care information security and privacy (listed here as health care security) are two of the optional areas that can be supported by our university. While the cyber investigations functional area, as initially documented, focuses primarily on digital forensics, it is envisaged that cyber intelligence will become an important component of this functional area as investigations become more proactive rather than reactive, leading to our specialty in cyber intelligence.

As an institution, we are focusing on the following three focus areas for our upcoming reaccreditation: cyber investigations, data security analysis, and health care security.

Department of Labor Competency Model

The Employment and Training Administration (ETA) of the Department of Labor (DOL) has worked with the Department of Homeland Security and federal agencies that contributed to the NICE framework to develop a comprehensive competency model for cybersecurity. A cadre of technical and subject matter experts from education, government, business, and industry also contributed to the development of the cybersecurity model. (www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx)

The DOL Cybersecurity Industry Model defines the latest skill and knowledge requirements needed by individuals whose activities impact cybersecurity. Strategically the proposed model incorporates competencies identified in the NICE framework and complements the framework by including both the competencies needed by the average worker who uses technology, as well as the cybersecurity professional. The ETA model (shown in Figure 4) will be updated to reflect future changes to the NICE framework.

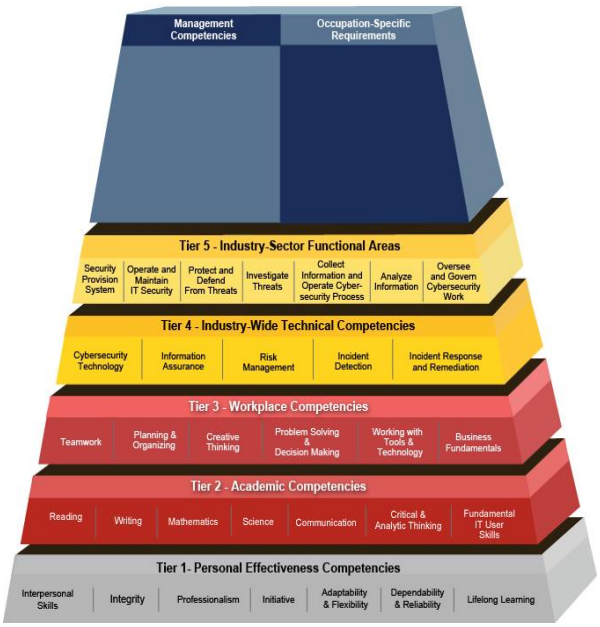

Figure 4. The DOL ETA model (Adapted from www.careeronestop.org)

The model shows general skill requirements as well as industry sector functional areas (Tier 5). These skill areas closely follow the NICE framework. The top tier allows for individual customization in both the managerial and organization specific-space.

Using the interdisciplinary resources of the institution

Institutions have several disciplines that are related to cybersecurity and its application. The CAE IA/CD redesignation requires cybersecurity to be "multidisciplinary within the institution" (www.iad.gov/NIETP). In our university, these disciplines include IT, management, economics, management science, criminal justice, politics, sociology, and forensic and legal psychology. As we consider specialties at the graduate level, we focused our interdisciplinary review to those programs that offer graduate programs in their individual disciplines.

Cybersecurity is located in the business school providing daily contact with the health care management (HCM) faculty as well as the management science faculty. We already have a dual degree in HCM and IT. Further, we have existing courses in health care informatics and the security and privacy of electronic documents. In addition, we are collocated with the forensic and legal psychology program and are collaborating with them in research and curriculum development, particularly for their new intelligence studies specialty.

We have proactively sought conversations about cybersecurity education with these disciplines, and the university in general, and have achieved a high-level of participation in our endeavors.

3. WHEN TO MAKE CURRICULUM CHANGES

The impetus for introducing the above three specialties in our MS in Cybersecurity program was based on input from our Cybersecurity Advisory Group as well as feedback from our students. We then invoked an existing curriculum development model. This "holistic" model provides IS/IT educators with strategic guidance as for "when" to introduce topics on emerging technologies and "how" to incorporate the new knowledge into an existing IS/IT curriculum (Liu & Murphy, 2012). As presented in Figure 5, the original model integrates seven "forces" as a foundation to inform valid decisions as to when changes in the IT/IS curriculum are needed.

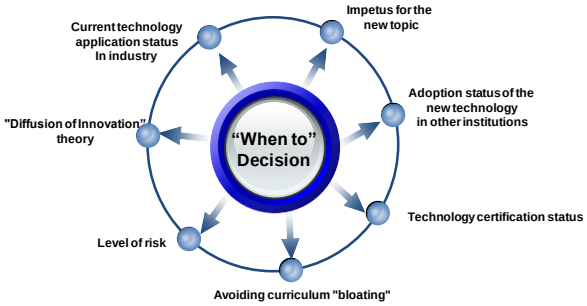

Figure 5. Strategic Model for Making "When" Decisions (Adapted from (Liu & Murphy, 2012))

The first factor is based on the widely cited "Diffusion of Innovation" theory and outlines the macro-level guidelines for the curriculum design, "*we must start early and keep exploring new topics and technologies, with credible leadership (i.e. across the department, the school, and the university) and have a competent team of faculty with the right expertise*" (Liu & Murphy, 2012, p.178)). Our location in the Washington, D.C. area provides us with an enviable adjunct faculty with extensive experience and knowledge.

The second factor is focused on the *current technology application status in industry*. The NICE and NIETP approaches emphasize the need for educators to consider "specialties", as dictated by the government need. DHS also promotes this specialization approach for private sector organizations, particularly those that are responsible for security and resilience of the nation's critical infrastructure elements (www.dhs.gov/critical-infrastructure). Finally, one of the important drivers for adding the data analysis specialty to the cybersecurity curriculum lies in its prevalence in a variety of sectors of industry and government. According to Gartner's survey of IT leadership, 42% of respondents stated they had invested in big data technology, or were planning to do so within a year (Gartner, 2013). This investment in the technology calls for an increase in recruitment of data scientists as has been reported extensively in the press. Our institution is in the Washington D.C. area and this is an important region for data analysis, in part because of the large number of data sources provided by the government and the increased focus of government agencies on data analytics, including in cybersecurity. Adjunct faculty are widely available and we did hire a data scientist as IT faculty in January 2014.

The third factor of the model is the *impetus for the new topic*. The stakeholders playing roles in the curriculum development process include faculty, students, advisory board members, accreditation bodies, and industry leaders (Liu & Murphy, 2012). The aforementioned example of the NIETP office updating its accreditation criteria to keep abreast with the state of the art of the cybersecurity discipline justifies, in part, our proposal of adding the three specialties to the cybersecurity program. In addition, the fact that students in the cybersecurity program have been showing interest in areas of intelligence studies, health care and data analysis is also one important indicator since they are one of major targets in the curriculum development process. Because of our location in the Washington DC metropolitan area, government careers are

significant possibilities for our graduates. This job market is important for our students and is one catalyst to introduce specialties to the curriculum.

The fourth factor incorporated in the model is the adoption status of the new technology topic in other institutions. Specializations in cybersecurity at the master's level are beginning to appear across the nation. For example, Ithaca College offers a cyber intelligence specialization in its online MS in cybersecurity program, including specific courses in topics such as cyber intelligence and domestic terrorism end extremist groups. (programs.online.utica.edu/programs/ms-cybersecurity-course.asp).

The availability of a certification in the technology by a reputable organization such as CompTIA or ISC^2 is also considered as an important factor in the model. For example, in information security, the Certified Information Systems Security Professional (CISSP) is considered as a critical certification for faculty and students in cybersecurity in general (Frank & Werner, 2011). The recent introduction of the Health Care Information Security and Privacy Professional (HCISPP) certification is considered an important driver for the health care security specialty.

The sixth factor in the model is a consideration of avoiding curriculum "bloating" This factor was important in our decision to introduce specialties to the cybersecurity program rather than increasing the credit requirements for the program. A course or program that is overloaded will result in high dropout rates and poor grades. An overarching inspection and management process are indispensable for the cohesiveness of the program.

The last factor in the model is the *level of risk*, including the complexity of the highly specific technology focused topics, the long turnover time of the curriculum approval process, and the cost associated with any equipment, software requirements, or library support needs for the new courses. The good relationship kept between the IT department and the other departments/programs, the frequent collaborations among faculty from the IT/IS department and the university curriculum committee, the continuing support from the National Science Foundation (NSF), and the availability of knowledgeable and experienced faculty, will make this curriculum development process smooth.

4. PLANNED CYBERSECURITY SPECIALTIES

The current MS in Cybersecurity program is 36 credits with eight core management and technical courses, three elective courses, and one capstone project. Students electing to take the specialty will take 39 credits with no electives. They will take 4 courses in the specialty area (replacing the 3 electives) and their capstone project must be in their specialty area. This provides them with 15 credits in their specialty area, including 3-credits that apply their specialty topic to either research or to a service project.

Cybersecurity Data Analysis

Cybersecurity data continues to grow within the government and private sector organizations. As the number of cybersecurity incidents grows, computer logs and monitoring tools, across a wide variety of network components and security devices, generate vast amounts of data. This data is mainly used for post-event analysis; once an attack has been detected, the investigation usually starts and the monitoring and log data is analyzed to identify the attack vector and the associated vulnerabilities; perhaps leading to finding who conducted the attack. However, the cybersecurity data could also be used for predictive analysis (cyber intelligence) whether for external attackers or for attacks from insiders.

The research company, Gartner estimates that data collected and stored by enterprise cybersecurity organizations will double through 2016 (Gartner, 2014). In addition, the "Internet of Things" will greatly increase the amount of data collected and stored as sensors and surveillance tools become ubiquitous (Gubbi, Buyya, Marusic, & Palaniswami, 2013).

Another factor to consider is the increasing emphasis on information sharing in cybersecurity. Traditionally, companies have held threat and vulnerability information close, rather than sharing it with each other or the government. However, recent actions, primarily by the DHS, have removed some of the impediments about information sharing particularly with respect to the critical infrastructure (Hayden & Zuckerman, 2012; Information Sharing Environment (ISE), 2013). Data stored in logs and other monitoring tools vary from operating system to operating system and from one vendor's security

management tool to another, resulting in variations in what is stored and how it is stored across organizations. This makes sharing detailed attack information for potential threats across the global landscape more difficult. In addition, organizations are combining their internally generated log data with additional information that can be obtained from public sources such as the Whois database and the DNS records. This is resulting in data stores that are not only of high volume but also of high variability.

If monitoring tools are to be used to prevent an attack or to quickly mitigate the effects, then time is of the essence and so data must be analyzed and visualized almost in real-time. As the velocity of the data becomes significant, particularly based on the "Internet of Things", the need for fast analysis is significant in the cybersecurity domain. Finally, the veracity (validity) of data is also a constant issue in cybersecurity, as exemplified by the decline in accuracy in the Whois database (including deliberately incorrect records and the invocation of the "privacy" option by some registrars) and the constant spoofing of source IP addresses.

There is recognition of the cybersecurity data analysis issue by some of the security management vendors and several "Security Information and Event Management" (SIEM) solutions have been introduced. These solutions mainly focus on the real-time analysis of security alerts generated by a range of hardware, software, and software devices in the enterprise network, by compiling and analyzing data in some centralized location (McAfee, 2013). In addition, there have been multiple studies on the use of data science in cybersecurity in the field. For example, in a recent study, the Ponemon Institute found that more than 80% of the organizations surveyed would like to see big data analytics combined with other security initiatives (Ponemon Institute, 2013).

Data science has become a major initiative in business, science and other fields to handle "big data" issues. While a data scientist has a strong background in computer science and mathematics, the major role of the data scientist is to sift through large amounts of data to discover previously hidden insights. As such, the data scientist must have skills in all phases of the data science process including data collection, data storage, data wrangling, data retrieval, data analytics, data mining, and data visualization. More importantly, a recognized component of successful data science is "domain" knowledge: the human intelligence that accumulates within a certain discipline. Domain expertise is necessary to genuinely understand how to apply data science effectively: for instance, to know which data, from all the possible sources, are valuable and which are not. Without the right domain knowledge, much time and effort is wasted in finding the right data instead of solving the most important problem(s).

The four proposed specialty courses include:

- **Data Management for Cybersecurity Information:** this course examines the collection and data and its integration into a database that can be used for subsequent data analysis. Big data techniques will be discussed including effective data collection, data validation, data wrangling, and database loading. Cybersecurity data sources will be used, including those available from the government or Internet sources.
- **Cybersecurity Data Analysis:** this course focuses on the statistical techniques available for different types of data analysis, emphasis being placed on how to apply the techniques rather than mathematical concepts. Students will be required to work with statistical tools and use the R programming language.
- **Cybersecurity Data Visualization:** this course focuses on the communication of results and examines the need to visually represent complex data for management consideration. Reporting, visualization and infographic techniques are explored and students will be expected to use visualization tools with cybersecurity data.
- **Special Topics in Cybersecurity Data Analysis:** this course will focus on new topics in the field and reflects anticipated changes in the cybersecurity data analysis discipline, including new sources of information and new analytical techniques.

Students will be then expected to apply these knowledge units in their capstone projects at the end of their program.

Cyber intelligence

The US Director of National Intelligence has ranked cybercrime as the top national security threat, higher than that of terrorism, espionage, and weapons of mass destruction (Director of National Intelligence, 2014). As today, not only common criminals, but also organized crime rings and nation states are taking a more active role in the cyber arena (Cyber Security Forum Initiative, 2014). Some of these agents have launched very sophisticated and targeted attacks that are hardly detectable (Mandiant Intelligence Center, 2013). A recent report by the PWC and the Software Engineering Institute (SEI) Computer Emergency Response Team (CERT) shows that organizations that have detected such incidents are more likely to employ security capabilities such as vulnerability management, cyberthreat intelligence analysis, intrusion detection tools, and SIEM technologies. (PWC, 2014).

As cybersecurity risks continue to escalate, it is imperative for organizations to move away from reacting (to incidents) to predicting and preventing them (Information Security Forum (ISF), 2012). Cyber intelligence plays a key role in analyzing current cyber incidents in order to predict the emerging threats. "The role of intelligence in any capacity is to collect, analyze, and produce information to provide complete, accurate, timely, and relevant threat assessments to inform decision makers… Effective cyber intelligence will begin to enable predictive, strategic warning regarding cyberthreat activities, mitigate risks associated with the threat, enhance our ability to assess the effects of cyber intrusion, and streamline cyber security into a more efficient and cost effective process based on well informed decisions" (Intellegence and National Security Alliance (INSA), 2011).

NICE Framework defines the required KSAs (Knowledge, Skills and Abilities) for a Cybersecurity Intelligence Analysis (under Category of "Protect and Defend" and the specialty area of "Computer Network Defense") as "Uses information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats." These are very much aligned with the traditional intelligence cycle, which is a circular and repeated process to collect and convert data into intelligence; and has the following five steps: planning and direction, collection, processing, production and dissemination (Department of Defense, 2013). Similarly, SEI has defined a cyber intelligence framework and an overview of this is presented in Figure 6. (www.sei.cmu.edu/about/organization/etc/citp-summary.cfm).

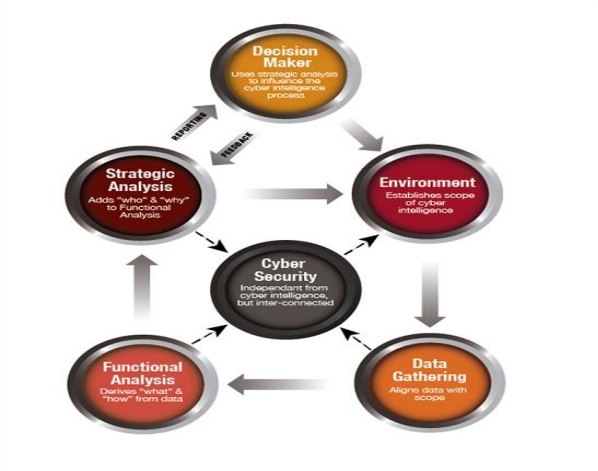

Figure 6: SEI Cyber Intelligence Framework (Adapted from sei.cmu.edu)

Considering the SEI framework (SEI Emerging Technology Center, 2013), the coursework for a specialty in cyber intelligence should cover the following KSAs.

- **Data gathering and examination:** Exploring a variety of manual and automated data sources, collecting information, aggregating and analyzing it through automated intelligence techniques.
- **Functional and strategic threat analysis:** Functional analysis focuses on answering the "what" and "how" of cyberthreats whereas strategic analysis aims to answer "who" and "why." Both analyses require advanced content knowledge and strong critical thinking skills.
- **Reporting for decision makers:** Dissemination of intelligence to decision makers through concise and accurate technical reports, and coordinate sharing of information with all involved parties.

Therefore, the cyber intelligence specialty will require the students to complete following four courses:

- **Intelligence Studies: this course examines the traditional fields of intelligence and examines how some of these tried and tested tools and techniques (including counterterrorism) can be applied to the cybersecurity field.**
- **Cyber intelligence: the course includes open-source intelligence (OSINT) tools, tactics, techniques, procedures (TTP) and indicators of compromise (IOC), motivation of adversaries, cyberprofiles and behaviors, situational awareness. The course also includes the legal parameters for cyber intelligence.**
- **Investigating cybercrimes: the course includes techniques such as the legal parameters for pursuing and prosecuting cybercriminals, communicating and collaborating with law enforcement and legal teams, as well as global considerations.**
- **Cyber counterintelligence: this course includes both defensive and offensive cyber counterintelligence techniques and strategies, reverse deception, cyber espionage, insider threats, and the use of data to predict potential incidents.**

The capstone project will include a detailed case study and the application of these techniques to the particular scenario.

Health Care Information Security and Privacy

The health care industry is facing an uphill battle in its efforts to detect and prevent cyber-attacks, and reduce and stop the loss or theft of protected health information (PHI) or patient information. According to a recently-published analysis of Standard & Poor's (S&P) 500-stock index companies by BitSight Technologies, health care and pharmaceutical companies rate lowest among finance, utilities, and retail in terms of security performance (BitSight Technologies, 2014). Another survey conducted by the Identity Theft Resource Center (ITRC) revealed that medical-related identity theft accounted for 43% of all identity thefts reported in the United States in 2013, which surpassed identity thefts involving banking and finance, the government and the military, or education (Identity Theft Resource Center, 2014). Ponemon Institute has conducted an annual benchmark study on patient privacy and data security since 2010. The third annual study reported that some 94 percent of medical institutions have been victims of a cyber attack (Ponemon Institute, 2012). Various reports show that cyberthreats are not declining. The most recent annual study discloses that criminal attacks on health care systems have risen a startling 100 percent since their first annual report in 2010, resulting from inadequate resources such as funding, technologies, trained personnel and expertise (Ponemon Institute, 2014).

Furthermore, "with the push to digitize all health care records, the emergence of healthcare.gov and an outpouring of electronic protected health information (ePHI) being exchanged online, even more attack surfaces are being exposed in the health care field" (Filkins, 2014, p.2). In April, 2014, the Federal Bureau of Investigation (FBI) warned health care providers that their cybersecurity systems are lax compared to other sectors, thus, may be more vulnerable to attacks by hackers searching for Americans' personal medical records and health insurance data, "The health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely" (Finkle, 2014).

The alarming facts of cyberthreat in the health care field reveal "how far behind industry-related cybersecurity strategies and controls have fallen" (Filkins, 2014, p.2). Obviously, there has been a great demand from the industry for health care IT personnel with adept security skills and knowledge, an important component of our curriculum adoption model.

As the technology certification status is another important factor in the adoption model, current certifications available in health care security and privacy by reputable organizations are examined below.
Two recent examples are:

- CompTIA Healthcare IT Technician: (certification.comptia.org/getCertified/certifications/hittech.aspx)
- AHIMA: Certified in Healthcare Privacy and Security (CHPS®): (www.ahima.org/certification/chps)

In addition, the International Information Systems Security Certification Consortium ((ISC)^2), the leader in educating and certifying information security professionals, launched a new certification, Health Care Information Security and Privacy Practitioner (HCISPP). The HCISPP is a demonstration of knowledge by security and privacy practitioners regarding the proper controls to protect the privacy and security of sensitive patient health information as well as their commitment to the health care privacy profession. The HCISPP Common Body of Knowledge (CBK) consists of the following six domains (www.isc2.org/hcispp-domains/default.aspx):

- Health care industry;
- Regulatory environment;
- Privacy and security in health care;
- **Information governance and risk management;**
- Information risk assessment; and
- Third-party risk management.

Taking both the CAE/ID focus areas and the available certifications, including the (ISC)^2 HCISPP CBK ((ISC)^2, 2013) into consideration, the four proposed specialty courses are listed as follows:

- **Introduction to the Health Care Industry**: this first course covers the basics of the health care environment including types of organizations, health insurance, coding, as well as function, structure, and financing of health care. It includes third-party relationship (e.g., vendors, data sharing, etc.) and health data interoperability and exchange.
- **Health Care Security and Privacy Policy**: this course focuses on applicable regulations, policies and compliance frameworks related to health information (e.g., data breach regulations, ePII, generally accepted privacy principles, etc.). Students will develop policies for the type of threats faced by facilities.
- **Privacy and Security of Electronic Documents**: this course focuses on the management of large volumes of documents (from images to test results, from prescriptions to insurance claims) in health care and discusses tools and techniques to protect security and privacy
- **Risk Management in Health Care**: The course discusses how organizations manage information risk through security and privacy governance. It includes risk identification, risk assessment, and mitigation actions. It also covers how to manage third party risks.

The final capstone project will focus on the application of security and privacy control to health care data, by either working with a case study or by service learning**.**

5. CONCLUSIONS

Cybersecurity is a fast growing discipline and there is a need for more educated and trained personnel who have a mastery of the subject matter. Educators need to take a strategic role in preparing this workforce and the need for cybersecurity specialties is one such strategy. Based on a holistic model, we have carefully examined the seven factors, which influence our decision to offer three specialties in our MS in Cybersecurity program: cybersecurity data analysis, cyber intelligence and health care security and privacy. As a small private university, we have looked outside our discipline to find resources that can supplement our technical cybersecurity knowledge and skills from other faculty teaching in related topics, and whose students may be interested in some of these overlapping courses.

6. REFERENCES

(ISC)^2. (2013). *HealthCare Information Security and Privacy Practitioner Exam Outline*.

Anderson, K. (2013). Building a Better Information Assurance Degree and Promoting Cybersecurity Education. *ISSA Journal, 11*(5), 20-23.

BitSight Technologies. (2014). Will Healthcare be the next Retail? Retrieved from http://www.bitsighttech.com/

Cyber Security Forum Initiative. (2014). Executive Cyber Intelligence Report. (June 3, 2014). Retrieved from http://www.tripwire.com/state-of-security/government/executive-cyber-intelligence-report-june-3-2014/

Department of Defense. (2013). Joint Publication (JP) 2-0: Joint Intelligence.

(October 2013). Retrieved from http://fas.org/irp/doddir/dod/jp2_0.pdf

Department of Defense. (2014). DoD 8570.01-M, Information Assurance Workforce Improvement Program, Change 3.

Director of National Intelligence. (2014). Worldwide Threat Assessment of the US Intelligence Committee. (January 29, 2014). Retrieved from http://www.dni.gov/index.php/newsroom/testimonies/203-congressional-testimonies-2014/1005-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community?tmpl=component&format=pdf

Filkins, B. (2014). Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon: SANS Institute.

Finkle, J. (2014). Exclusive: FBI warns healthcare sector vulnerable to cyber attacks. Reuters. Retrieved from http://www.reuters.com/article/2014/04/23/us-cybersecurity-healthcare-fbi-exclusiv-idUSBREA3M1Q920140423

Frank, C., & Werner, L. (2011). *The Value of CISSP Certifocation for Educators and Professionals.* Paper presented at the Information Security Curriculum Development Conference, Kennesaw, GA

Gartner. (2013). Gartner Survey Finds 42 Percent of IT Leaders Have Invested in Big Data or Plan to Do So Within a Year. Retrieved from http://www.gartner.com/newsroom/id/2366515

Gartner. (2014). Predictions 2014: Garner's Predictions for the Year Ahead. Retrieved from http://www.acq.osd.mil/dsb/reports2010s.htm

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future Generation Computer Systems 29*(7), 1645-1660

Hayden, M., & Zuckerman, M. (2012). Cybersecurity Task Force: Public-Private Information Sharing. Bipartisan Policy Center. Retrieved from http://bipartisanpolicy.org/library/report/cybersecurity-task-force-public-private-information-sharing

Identity Theft Resource Center. (2014). 2013 ITRC Breach Report. Retrieved from http://www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html

Information Security Forum (ISF). (2012). Data Analytics for Information Security, from Hindsight to Insight. Retrieved from https://www.securityforum.org/research/

Information Sharing Environment (ISE). (2013). 2013 Annual Report to the Congress. Retrieved from http://www.ise.org/annualreport

Intellegence and National Security Alliance (INSA). (2011). Cyber Intelligence: Setting the landscape for an emerging discipline. (September, 2011). Retrieved from http://www.insaonline.org/i/d/a/resources/Cyber_Intelligence.aspx

ITU-T. (2014). X.1205, Overview of cybersecurity. Retrieved from http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Liu, X., & Murphy, D. (2012). *Tackling an IS Educator's Dilemma: A Holistic Model for "When" And "How" to Incorporate New Technology Courses into the IS/IT Curriculum* Paper presented at the Proceedings of the Southern Association for Information Systems Conference, March 23rd-24th, 2012, Atlanta, GA.

Mandiant Intelligence Center. (2013). Mandiant Intelligence Center Report: APT1: Exposing One of China's Cyber Espionage Units. (February 18, 2013). Retrieved from http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

McAfee. (2013). SIEM: Keeping Pace with Big Security Data. CIO Magazine White Paper.

Ponemon Institute. (2012). The Third Annual Benchmark Study on Patient Privacy and Data Security. Retrieved from http://www.ponemon.org/news-2/45

Ponemon Institute. (2013). Big Data Analytics in Cyber Defense. Ponemon Institute Research Report. Retrieved from http://www.ponemon.org/library/big-data-analytics-in-cyber-defense

Ponemon Institute. (2014). The Fourth Annual Benchmark Study on Patient Privacy and Data Security. Retrieved from http://www.ponemon.org/blog/fourth-annual-benchmark-study-on-patient-privacy-and-data-security

PWC. (2014). US cybercrime: Rising risks, reduced readiness-Key findings from the 2014 US State of Cybercrime Survey. (June, 2014). Retrieved from http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

SEI Emerging Technology Center. (2013). Cyber Intelligence Tradecraft Project, Summary of Key Findings. (January 2013). Retrieved from http://www.sei.cmu.edu/library/assets/whitepapers/citp-summary-key-findings.pdf

Woener, R. (2012). Security Education vs Training. *Information Security, 14*(4), 6-7.