# An Interdisciplinary Approach to Cybersecurity Curriculum

**Donna M. Schaeffer**
**Marymount University**

**Patrick C. Olson**
**National University**

**Cynthia Knott Eck**
**Marymount University**

*Today's global information systems are inter-related and inter-dependent. Attacks on a single institution in one country can have major impacts throughout the world. Collaborative efforts by the United States Government and private sector led to the development of a voluntary risk-based Cybersecurity Framework, a set of broad standards and best practices that work across industries. The Framework avoids placing additional regulatory requirements on businesses. The Framework can serve a model for designing curriculum and developing cybersecurity courses. It provides a good vehicle for bringing interdisciplinary aspects into the curriculum.*

## CYBERSECURITY

As an academic discipline, cybersecurity knowledge grew out of computer security in the fields of information systems, information technology, and computer science. Today, it is a broad field that is both interdisciplinary because it relates to more than one branch of knowledge and multidisciplinary, by virtue of combining or involving several academic disciplines or professional specializations in an approach to a topic or problem. Indeed, cybersecurity may be best described as "transdisciplinary" in which study and research cross many disciplinary boundaries and takes a holistic perspective. In this paper, we will use the term interdisciplinary to describe interdisciplinary, multidisciplinary or transdisciplinary.

### Cybersecurity in the News

The breadth of news stories about cybersecurity show the interdisciplinary nature of the field. Recent examples that highlight the importance of cybersecurity were taken from a one-week time period in 2016. The Federal Bureau of Investigation (FBI) warned the automotive industry about vehicle hacking risks (Reuters, 2016). In 2015, Fiat Chrysler Automobiles NV recalled over a million vehicles to install anti-hacking software, GM issued a security update for its mobile application that allows owners to open doors and start the engines of some models, and BMW soon followed suit.

In finance, The Financial Times (2016) reported that revenues for Paysafe PLC, a global online payments system, grew 68% in one year. Its business model includes prepaid cards and digital wallets. The financial industry demonstrates the global issues. For example, the FBI helped in a case where over

$950 million was transferred from the Federal Reserve Bank in NY to three casinos in the Philippines (Quadir, 2016). The transfer order originated in Bangladesh, and after revealing the User IDs involved in the heist, an employee in the information technology department at Bangladesh's Central Bank was kidnapped and subsequently found physically unharmed.

Social media, especially celebrity and entertainment accounts have experienced security breaches. Blankstein (2016) reported on a Pennsylvania man who pled guilty to hacking celebrities' email and iCloud accounts. The breaches came to light when nude photos of a celebrity were published. These photos were on her iPhone and stored in the cloud.

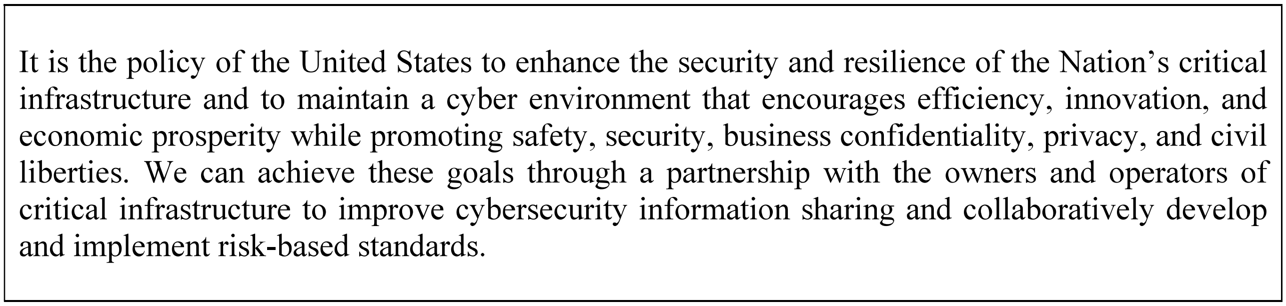
Although North Korean officials denied hacking into the mobile phones of 40 South Korean national security officials and the email accounts of railway employees, other countries don't believe the denials (Munroe, 2016).

These few examples from a one-week time period in 2016 show that cybersecurity is a concern in many fields, and subject area expertise in diverse fields like engineering and finance, among others, is needed. Additionally, cybersecurity is a global issue; thus, knowledge of international relations and policy is critical.

## United States Executive Order

In 2013, then-President Barack Obama signed Executive Order 13636 Improving Critical Infrastructure Cybersecurity. Figure 1 shows the introduction of the order.

**FIGURE 1**
**EXECUTIVE ORDER 13636 IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY**



It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

The order provides for new information sharing programs to provide both classified and unclassified threat and attack information to U.S. companies and the development of a Cybersecurity Framework. It also includes strong privacy and civil liberties protections based on the Fair Information Practice Principles, establishes a voluntary program to promote the adoption of the Cybersecurity Framework, and calls for a review of existing cybersecurity regulation.

Critical infrastructure includes both physical and non-physical systems and assets that fundamental to day-to-day security, economic functioning, and/or public health and safety. The incapacity or destruction of these systems or assets could be devastating to the society at large. The Department of Homeland Security has identified 16 industries as comprising the critical infrastructure: chemical, commercial facilities (e.g., shopping centers and sports /entertainment venues), communications, some manufacturing, dams, defense, emergency services, energy, financial services, food and agriculture, government facilities, health care and public health, information technology, nuclear reactors/materials/waste, transportation, water and wastewater systems.

The order tasks the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence to produce unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity on a timely basis. Classified reports may also be shared with organizations on a need-to-know basis. It also requests organizations in the critical infrastructure sectors to voluntarily provide information about threats they have received.

The National Institute of Standards and Technology began development of a Cybersecurity Framework in 2014. The purpose is to provide principles and best practices for security, resilience, and risk management. It considers business requirements, risk tolerances, and resources and recognizes the unique risks that various organizations and industry sectors face. A draft of the Framework was made public in 2017.

The increasing frequency and depth of cybersecurity attacks and the establishment of the Framework make it clear that there is a cybersecurity workforce skills gap in the United States.

## CYBERSECURITY WORKFORCE SKILLS GAP

In an interview on NPR (Gjelten, 2010) James Gosler put the number of qualified cybersecurity personnel at just 1,000 in the entire United States. To meet the computer security needs of U.S. government agencies and large corporations, he estimated a need for a workforce of 20,000 to 30,000 skilled specialists. The United States is not the only country with a workforce skills gap. A report from the United Kingdom (National Audit Office, 2013)(National Audit Office, 2013) indicates it could take up to 20 years to train enough qualified cybersecurity experts.

The workforce skills gap is a multi-layered issue. First, as noted above there is a shortage of skilled applicants. However, there are two additional aspects to the skills gap problem. In addition to there being so few qualified applicants, among those "qualified" applicants as few as 25% of the applicants are qualified to handle the work (Richards, 2015). One of the important causes of this problem is that advanced threats and malware are continuously changing; thus staying current in this field is very difficult. This need for current knowledge creates another additional problem. In effect, once someone is in place at a job, there is a need to keep their skills up to date and that is not happening (Oltsic, 2014). A recent presentation at the RSA Conference about a study of 315 Cybersecurity Professionals at companies with over 1,000 employees. Four major deficiencies were identified.

Before examining these deficiencies, it is important to keep the following in mind: First, the personnel shortage in Cybersecurity is somewhat different from the longstanding Information Systems, Information Technology or Computing personnel shortage. Two important differences are that IS, IT and Computing can vary depending on the "strategic" importance to the enterprise (Cybersecurity mitigates risk which necessarily means less variance). Second, IS, IT and Computing tend to build tools that help offset their personnel shortages. Cybersecurity is necessarily responding to "unknown" threat which cannot be addressed in advance.

The deficiencies of current Cybersecurity staff occur in four very important areas. These are Command & Control communication techniques, polymorphic malware, metamorphic malware, and zero-day malware. Specifically, fifty percent of the security professionals were not ready on Command & Control communications techniques. Forty percent of the security professionals were not ready on polymorphic malware. Forty percent of the security professionals were not ready on metamorphic malware. Twenty-nine percent of the security professionals were not ready on zero-day malware (Oltsic, 2014).

These deficiencies occur in the commonly needed parts of the field and not in the esoteric and less needed domains. Command & Control Communications techniques refers to how compromised systems are operated by hackers. A commonly used approach is referred to as a "heartbeat." A program is embedded in a computer and it communicates via the heartbeat with a remote machine that provides it with instructions and updates. Using the "heartbeat" technique, the communication will be undiscovered and there will be no indication of a problem until the embedded software finally makes an attack. The knowledge required in this case is the mechanism that is used for this attack, which should be protected with safeguards.

Metamorphic malware refers to virus, worm, Trojan, spyware that avoids detection by changing the main body of the program. Change is accomplished thru encryption of the malware's software body and a separation of the decryption process (which contains the key) into a separate unit. This allows the malware software to encrypt itself when propagating, in the case of metamorphic software this change is to the body of the software code rather than the decryption process. Thus, a mere list of threats won't work, because the threat looks different after each generation. Polymorphic malware does not change the body of the malware software but does change the decryption process. The part of the threat that contains the key also contains a mutation generator to randomize the variables that the mathematics uses. The result is that the key for the next generation of threats is more difficult to predict. The knowledge needed here is about these types of threats and the need to make sure that systematic changes to the organizations "defensive" process are taking place at least provide detection (Sharmo, 2014).

Zero-day refers to vulnerabilities in software that vendors do not know about and have therefore not addressed. It is hoped that the detail provided in the prior paragraph gives a sense of how zero-day would be different problem. From the preceding discussion, the number of possible ways to create threat software is very, very large. Thus, predicting the attributes of new threats is unlikely. The knowledge needed is in part knowing about the community of practice that is constantly trying to identify new software threats and can be had, in part, by keeping up with the news about new software threats.

These four deficiencies are challenging for those who wish to keep current. However, in many respects they define what Cybersecurity is supposed to be doing. Thus, these deficiencies and the attributes of the practitioners in this field are very important.

### The National Cybersecurity Workforce Framework.

The National Institute of Standards and Technology (National Institute of Standards and Technology, U. S. Department of Commerce, 2017) devised a cybersecurity workforce framework originally for the federal sector, but it can be used by any sector. It can be used to identify workforce gaps and to write position descriptions. The framework specifies the knowledge, skills, and abilities required in various cybersecurity positions. It provides a solid foundation for developing curriculum and designing courses.

The workforce framework comprises seven areas: 1) securely provision, 2) operate and maintain, 3) protect and defend, 4) investigate, 5) collect and operate, 6) analyze, and 7) oversight and development.

Used as a basis for designing curriculum in Cybersecurity, the NIST framework yields an interdisciplinary curriculum. The discipline of Accounting contributes topics like auditing and control. There is also a contribution of techniques, for example, cost-benefit analysis can help cybersecurity professionals make decisions about systems. The discipline of cybersecurity may learn lessons from the field of Forensic Accounting. This is a relatively young specialized discipline that has evolved as technology advanced.

The financial industry is considered a critical infrastructure, which ensures connection between Finance and cybersecurity. The field of Finance adds topics such as risk management to the cybersecurity discipline.

Knowledge of law and regulation is essential for cybersecurity professionals.

The Marketing and Communications disciplines are also important to cyberseecurity. Marketing collects data, which must be kept secure. Such data presents a big risk as a entry for cyber-attacks. Cybersecurity professionals may have to communicate with their staffs, their counterparts in other agencies and organizations, and even the public.

Cybersecurity is at the forefront of international relations. An understanding of global issues is critical for cybersecurity professionals.

## CONCLUSION

It takes a village to educate cybersecurity professionals. This is directly the result of the "transdisciplinary" nature of the field. That is, this field requires knowledge from a variety of disciplines to be effective. Thus, the students can possess different undergraduate degrees and the faculty can represent a range of disciplines. Students, faculty, and the field of cybersecurity are brought together via the NIST framework described above. Cybersecurity education is a dynamic field, which can be challenging.

## REFERENCES

Blankstein, A. (2016, March 15). *Pennsylvania Man Is Charged in Celebrity Hack, Reaches Plea Deal.* Retrieved August 13, 2017, from nbc.com: http://www.nbcnews.com/tech/tech-news/pennsylvania-man-arrested-will-plead-guilty-celebrity-hacking-n539166

Gjelten, T. (2010, July 19). *National Security: Cyberwarrior Shortage Threatens U.S. Security.* Retrieved August 13, 2017, from npr.org: http://www.npr.org/templates/story/story.php?storyId=128574055

Munroe, T. a. (2016, March 12). *North Korea denies cyber attacks on South Korea officials.* Retrieved August 13, 2017, from reuters.com: http://www.reuters.com/article/us-northkorea-korea-cyber-idUSKCN0WF05V

National Audit Office. (2013, February 12). *ICT and systems analysis:.* Retrieved August 13, 2017, from The UK cyber security strategy: Landscape review: https://www.nao.org.uk/report/the-uk-cyber-%20security-strategy-landscape-review/

National Institute of Standards and Technology, U. S. Department of Commerce. (2017, April 4). *The National Cybersecurity Workforce Framework.* Retrieved August 13, 2017, from csrc.nist.gov: https://www.nist.gov/sites/default/files/documents/2017/04/04/national_cybersecurity_workforce_framework_03_2013_version1_0_interactive.pdf

Oltsic, J. (2014, January 24). *The Cybersecurity skills gap is worse than you think.* Retrieved August 12, 2017, from CSO Online: http://www.csoonline.com/article/2226178/cisco-subnet/the-cybersecurity-skills-gap-is-worse-than-you-think.html

Quadir, S. (2016, March 20). *World: Bangladesh gets FBI help on bank heist; cyber-expert missing.* Retrieved August 13, 2017, from washingtonpost.com: https://www.washingtonpost.com/world/bangladesh-gets-fbi-help-on-bank-heist/2016/03/20/375f6f0c-eedb-11e5-89c3-a647fcce95e0_story.html?utm_term=.5872502c6c4d

Reuters. (2016, March 17). *Hacking: FBI Warns Automakers, Owners About Vehicle Hacking Risks.* Retrieved August 13, 2017, from Fortune.com: http://fortune.com/2016/03/17/fbi-warns-automakers-hacking/

Richards, K. (2015, August). *News: Cybersecurity Skills Shortage Demands New Workforce Strategies -- The race to find InfoSec professionals who can outpace advanced threats has companies worldwide facing hurdles.* Retrieved August 12, 2017, from TechTarget SearchSecurity: http://searchsecurity.techtarget.com/feature/Cybersecurity-skills-shortage-demands-new-workforce-strategies

Sharmo, A. a. (2014). *Evolution and Detection of Polymorphic and Metamorphic Malwares: A Survey.* Retrieved August 13, 2017, from arixiv.org: https://arxiv.org/ftp/arxiv/papers/1406/1406.7061.pdf

The Financial Times. (2016, March 16). *Paysafe Group PLC, Final Results.* Retrieved August 13, 2017, from ft.com: https://markets.ft.com/data/announce/full?dockey=1323-12738962-1UROAT2OLEKQKFI5JFFS90ETD8