Quality Assurance in University Cybersecurity Education

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

David Martin Salzberg

Spring, 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature ____ Date __________

Martin Salzberg

Approved ____ Date __________

MC Forelle, Department of Engineering and Society

INTRODUCTION

As society's infrastructures become more reliant on technology, it is necessary to consider how those technologies themselves, like computer systems, need to be protected in order to protect their corresponding infrastructures in turn. If precautions aren't taken when such technologies are implemented, it could lead to large-scale consequences depending on the context when a security failure occurs.

For instance, in 2021, attackers took advantage of a vulnerability and hacked into the Colonial Pipeline, which is a pipeline that spans 5,500 miles along the east coast of the United States and supplies nearly half of all fuel for the east coast. During the attack, a hacker group called DarkSide stole 100 gigabytes of data and infected many of the pipeline's IT computer systems with ransomware (Kerner, 2022). In order to prevent the attackers from causing more damage, the Colonial Pipeline shut down the pipeline for several days (US Dept. of Energy, 2021). As a result, the shutdown of the pipeline caused fuel shortages and price spikes along the east coast, which led to panic along the east coast due to its significant fuel supply. The shutdown largely caused disruptions in businesses, government, and individuals in the affected regions since the fuel shortages and panic led to long lines at gas stations, some of which even ran out of fuel entirely, inhibiting some people's transportation if they needed to travel for work (Sanger & Perlroth, 2021). The pipeline remained locked down until the Colonial Pipeline paid the attackers 75 bitcoin ($4.4 million) as ransom so the pipeline could resume its operations. The security breach occurred as a result of an employee's password leak, which gave the attackers access into the Colonial Pipeline's corporate network (Kerner, 2022). The coverage of the attack highlighted the significance of a vulnerability in critical infrastructure (Bhaiyat & Sithungu, 2022).

The previous case is an example of a ransomware attack, where data is stolen, encrypted, and held hostage until its ransom is paid. Ransomware attacks are just one type of attack, of which there is a large variety, which makes it difficult to implement security systems to prepare for attacks ahead of time. As a result, there are several things to consider during a security system's implementation, leading to multiple methods and styles of detection to protect a system's software. In general, there are two main ideas that are considered for detection of an intrusion: blacklisting known malicious activity, or developing a model of known safe activity and flagging activity outside that model, also known as whitelisting (Hassan, 2022).

Additionally, it is impossible to protect against never-before-seen attacks, also known as zero-day attacks, which limit the options to a reactive defense (Roumani, 2021). Zero-day attacks take advantage of a previously unknown software vulnerability, so by nature they can't be prepared for beforehand. Although it is impossible to prevent a cyber-attacker from exploiting a zero-day vulnerability, it is possible to learn to create robust technology and establish strong techniques that match the state-of-the-art practices used in industry to best prepare and protect against known, documented attacks while simultaneously looking towards the future.

To encompass the quality of how standard cybersecurity practices are taught, this research intends to bring attention to the responsibility of cybersecurity educators to ensure that their students acquire and apply the security skills they may use in the workforce. The literature review discusses some of the current standards of cyber defense and the possible consequences of a failure to implement them. Additionally, it covers education and its role in the context of cybersecurity, establishing how an increase in complexity in emerging technology makes its protection more complex as a result. I will conduct interviews with cybersecurity professors at the University of Virginia (UVA) to determine their main focuses considering their own approaches to teaching about the subject of cybersecurity in class. By interviewing cybersecurity educators about their teaching methods within the topic of security, I can learn which topics and teaching techniques they prioritize. I will utilize Star's infrastructure framework to analyze the data gathered within the interviews. Through the analysis of the information gathered in the interviews, I found that the professors discuss techniques and concepts that emphasize the significance of human error, adversarial thinking, and role of emerging technologies in the future of cybersecurity. Based on the analysis, I will conclude how cybersecurity educators ensure that their students are learning current best practices in cybersecurity. Through the techniques taught in their classes, cybersecurity educators aim for their students to critically think about security practices in the past, present, and future to best protect organizations, governments, and themselves against cyber-attacks.

LITERATURE REVIEW

The damage done by a cyber-attack could shut down some of the most critical parts of society's infrastructure, such as in the aforementioned Colonial Pipeline attack, so in an effort to mitigate the possible magnitude of damage done by a cyber-attack, there exist security standards that organizations should meet as a means of protection to everyone involved with each organization (Al-Zahrani, 2022; Bedi et al., 2021), but there have been some that have been too slow or failed to keep up with those standards, increasing the possibility of an attack. One of the most common sources of failure has to do with the level of security training given to employees by not teaching them how to safely do their work, as a security breach could easily occur by something as simple as opening an email (Abdalla et al., 2021). In the case of the Colonial Pipeline, it was an employee's failure to secure a password that gave the attackers access to its internal systems, which led to severe damages as described above.

Although known attacks are much more likely to be prevented once they have been discovered, zero-day attacks present a greater danger because security systems cannot be prepared for them beforehand. As a result, cyber-attacks occur on a regular basis, such as in the case of the Sophos XG Firewall, where a vulnerability allowed for attackers to inject their code into the firewall database with SQL injection, which exploits the SQL data storage software to gain access to and modify data stored in the database (Narang, 2020). This case suggests how even software designed to protect against attackers can be targeted, which indicates how the complexity of a technology can complicate its own protection mechanisms.

In order to minimize the chances of a cyber-attack happening when it could have been avoided, common weak points found throughout the history of cyber-attacks should be identified. According to a study by the State University of New York at Albany (2018), the weakest link in protecting cyberspace is not the technology; it is the human actors who commonly fail to defend against cyber-attacks. People's recklessness regarding their sensitive information like passwords is oftentimes the reason a malicious actor gains access to a computer system and can exploit that access to then cause further damage to an individual or an organization. For this reason, there is a level of social intelligence required to maintain a safe, protected environment in regard to a computer system.

Given the possible danger that a person's carelessness presents to a computer system, it becomes evident that cybersecurity is no longer as simple as having a high level of technical skill. Not only do cybersecurity professionals have to deal with the intricacies of the systems they work with every day, but they also must provide some degree of security training for the intended end users of the system who may not have the same level of security expertise (Dawson & Thomson, 2018). There is a variety of training techniques for employees that organizations commonly use today to protect their computer systems, some of which involve awareness of phishing scams, malware, and social engineering. As a result, the trained employees are less likely to reveal sensitive information that could be exploited by a cyber attacker.

Although the threat of cyber-attacks is ever-present to individuals and organizations, there is a degree of preparation that can be provided to university students before they enter the workforce. By giving the students some exposure to the notion of cyber-attacks while they are still in school, they will have gained experience that will help them later in their careers that can relieve some of the heavy-lifting and stress that organizations undergo when training their employees about cybersecurity, and that knowledge that the students gain can be applicable in any field in which they decide to work (Schneider, 2013). When weighing the possible benefit of previous training in cybersecurity, universities must consider how to instruct their students in the best practices available in industry standards.

There are two common approaches to university education in cybersecurity: instruction in principles and abstraction, and instruction in adversarial thinking. If educators prioritize principles and abstraction, there is more of a focus on teaching their students about developing defense systems. Students taught in principles and abstraction will have the tools to create robust, secure computer systems based on the core principles taught in their classes. Alternatively, if there is an emphasis on adversarial thinking, then the educators will teach their students how to think like a cyber-attacker. The reasoning behind teaching adversarial thinking is that the students will intrinsically learn cybersecurity measures once they recognize a security vulnerability in a computer system (Tagarev, 2019). There are benefits and tradeoffs for either option, so there have been debates among universities about the best teaching method for the topic, but there has not been a definite conclusion on the best teaching approach (Schneider, F., 2013).

STS FRAMEWORK

To analyze how professors account for future attacks by employing quality security education, I will employ Star's (1999) infrastructure framework, where technical systems are treated as infrastructures, even those outside the traditional idea of an infrastructure like roads and water systems. To that end, Star likens the idea of infrastructure to a part of human organization, serving as systems that function in the background to provide assistance in different fields of practice. The framework has a particular focus on the relations between infrastructures and people because an infrastructure could have different meanings and purposes to different people, and thus has a varying level of scalability depending on the infrastructure's context (Star, 1999).

Key concepts of infrastructures that are relevant to the topic of this project are embeddedness, reach or scope, embodiment of standards, and visibility upon breakdown. An infrastructure's embeddedness refers to the way it has sunk into the norms of society and the way it is perceived as a whole. Computers, computer networks, and information technologies are oftentimes lumped together as part of computer systems and the Internet as a whole, where in reality, different devices with different purposes could have varying effects of varying scale on different parts of society. Reach or scope has to do with how an infrastructure has reach beyond a single event or a one-time use, and the Internet has certainly stretched its bounds to civilizations around the world. Embodiment of standards defines an infrastructure's scope and limitations in order to access other infrastructures in a standardized fashion. Cybersecurity standards have become necessary in modern society in order to protect other critical infrastructures that could have severe consequences if they were to be attacked. Finally, visibility upon breakdown highlights how the invisible functions of an infrastructure suddenly become visible once the infrastructure breaks down, which is especially relevant since the prevalence of the Internet often leads it to be taken for granted, and it is forgotten how embedded it really is in daily life. For example, in the case of the Colonial Pipeline, there were American drivers on the east coast who panicked when the source of their transportation, which they had come to rely on, was threatened (Star, 1999).

METHODS

To research the ways cybersecurity educators teach best security practices, I will conduct interviews with professors at the University of Virginia who teach or have taught courses related to cybersecurity as primary sources. Within the interviews, I will ask the professors about how they teach the topic of cybersecurity to students in their own classes, which will provide insight on the preferred teaching approach on the topic at the university. Additionally, I will ask them about future emerging trends and technologies to study how they anticipate the ways in which their students' interactions with the technologies will have an impact on the future of cybersecurity.

The reasoning behind using university professors as a primary source of information for the purpose of this project is because of their direct interaction with their students, who take the information learned in class to use for the rest of their careers after graduation. Depending on the quality of education provided by those professors, their students may or may not enter the workforce with the knowledge to employ best practices in cybersecurity.

ANALYSIS

One of the common key factors involved in the occurrence of a cyber-attack mentioned among the interviewed professors was the vulnerability of human error revealing sensitive information that a cyber-attacker could exploit for further damage. If an attacker gains possession of an individual’s account password on a website, the attacker could have the capability to access the individual's personal information stored within the account. The attacker then has the ability to further try that password on other websites that contain more sensitive information such as credit card information, address, or even physical location. Furthermore, the access to that sensitive information could lead to blackmail, fraud, and theft. One such instance of a failure to protect information is that of the cyber-attack on the Colonial Pipeline mentioned beforehand, which is commonly presented to students as a case study of a historical cyber-attack in the professors’ classes. In this case, it was an employee’s careless password management that led to a cyber-attack that caused large-scale damage to critical infrastructure and lasting consequences on transportation infrastructures and the economy.

When I asked the professors about their own teaching approaches to the topic of cybersecurity, the most emphasized and common method was to first teach their students how to be an adversary. In the world of cybersecurity, learning to be an adversary refers to adopting the mindset of a cyber attacker, so the professors first teach cybersecurity students about different types of significant cyber-attacks and how to implement them. As an after-product, the students gain the hands-on knowledge of the capabilities and limitations of cyber-attacks, and can then produce code that takes those cyber-attacks into consideration which helps them design and create more robust, high-quality, and safe software as they enter the workforce after graduation.

Along the same lines, the level of preparedness that a student trained in cybersecurity principles and abstractions is lower than that of a student trained in adversarial thinking. If a student only focuses on historical events, their training will lack a significant portion of learning material: the future (Schneider, 2013). Following suit, the student will move forward in their career only with the knowledge of past events by not thinking like an adversary, which could leave critical backdoors open for cyber attackers to exploit.

Near the end of the interviews, I questioned the professors about their thoughts on emerging technologies and their roles in the future of cybersecurity. Because this portion is the most speculative part of the interviews, I recognized that there would be less consistency among each of their responses. As expected, the professors began to stray away from each other's opinions likely because of their differing specialties and interests rather than current trends. For instance, one professor who specializes in computer networks mentioned the latest in cellular technology: 5G networks. The spread of 5G mobile networks around the world has the capability to create stronger connections between people, machines, and Internet of Things (IoT) devices. Another professor mentioned the novel use of artificial intelligence in the development of new applications and devices. Even though the topic of this question is more open-ended than previous topics, it is still relevant to the purpose of this study because it is their students who will be developing and interacting with the new trends and technologies during their own careers.

CONCLUSION

Looking towards the future is becoming increasingly important in the context of cybersecurity as both cyber-defenses and cyber-attacks become more sophisticated over time, and the field of research is most likely to provide that lens, mitigating the damage caused by future attacks. Ideally, the work presented in this paper is aimed at professors, students, and even employers who have an interest in designing future-proof cybersecurity technology and techniques.

Past the scope of this project, future work could involve experiments with the quality of cybersecurity knowledge in students who have been trained in adversarial thinking versus those who are trained in principles and abstractions. By doing so, there may be an indication of the better practice between the two, or most likely different applications for which each type of training is better suited since cybersecurity, like other disciplines, does not have a one-size-fits-all solution to cyber-threats (Guttman, 2020). Regardless, it should be emphasized that any approach to an education in cybersecurity is better than none at all. Granted that the greatest vulnerability to a computer system is not the technology itself, but rather the humans who have access to it, there is a degree of urgency to prioritize training of the personnel who interacts with the technology over the complexity of the technology itself.

Furthermore, the trend of the rapidly occurring emergence of new technologies suggests that there will be new vulnerabilities associated with them, and new cyber defense techniques following suit. The possibility of such unforeseen technologies existing one day is becoming increasingly tangible as research in adjacent fields has made recent breakthroughs, such as those related to artificial intelligence and computer networks, so it is of the utmost importance that the quality of cybersecurity education provided to students and employees meets the standards of the best practices currently used in the industry.

REFERENCES

Abdalla M., Jarrah M., Abu-Khadrah A. & bin Arshad, Y. (2021). Factors Influencing the Adoption of Cyber Security Standards Among Public Listed Companies in Malaysia. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 12(11), 804-810. http://dx.doi.org/10.14569/IJACSA.2021.0121191

Al-Zahrani, A. (2022). Assessing and Proposing Countermeasures for Cyber-Security Attacks. *International Journal of Advanced Computer Science and Applications*, 13, 885-895. http://dx.doi.org/10.14569/IJACSA.2022.01301102

Bedi, P., Boyal, S. B., Kumar, J., & Ritika (2021). Cyber Security Management Model for Critical Infrastructure and Improving the Security Level on Transferring Digital Data. *Innovations in Bio-Inspired Computing and Applications*, 1372, 525-534. https://doi.org/10.1007/978-3-030-73603-3_49

Bhaiyat, H. Y. & Sithungu, S. P. (2022). Cyberwarfare and its Effects on Critical Infrastructure. *Proceedings of the International Conference on Information Warfare and Security (ICCWS)*, 2022, 536-543. https://doi.org/10.34190/iccws.17.1.68

Dawson, J. & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology*, 9. https://www.frontiersin.org/articles/10.3389/fpsyg.2018.00744/full

Guttman, R. (2020). How to Secure Electronic Data and Communications [Powerpoint Slides]. Carnegie Mellon University. Retrieved from https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/AD1110438.xhtml

Hassan, W. (2022). Malware. University of Virginia. Retrieved from https://collab.its.virginia.edu/access/content/group/217d57a4-19f8-4b04-b41d-9c43017ea817/Slides/CS4630-Fall2022-Lec12.pdf

Kerner, S. (2022). Colonial Pipeline hack explained: Everything you need to know. Tech Target. Retrieved from https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Narang, S. (2020). CVE-2020-12271: Zero-Day SQL Injection Vulnerability in Sophos XG Firewall Exploited in the Wild. tenable. Retrieved from https://www.tenable.com/blog/cve-2020-12271-zero-day-sql-injection-vulnerability-in-sophos-xg-firewall-exploited-in-the-wild

Office of Cybersecurity, Energy Security, and Emergency Response (2021). Colonial Pipeline Cyber Incident. US Department of Energy. Retrieved from https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

Roumani, Y. (2021). Patching zero-day vulnerabilities: an empirical analysis. *Journal of Cybersecurity*. Retrieved from https://academic.oup.com/cybersecurity/article/7/1/tyab023/6431712?login=true

Sanger, D. & Perlroth, S. (2021). Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity. *New York Times*. Retrieved from https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html

Schneider, F. B. (2013). Cybersecurity Education in Universities. *IEEE Security & Privacy, 11*(4),

3-4. https://doi.org/10.1109/MSP.2013.84

Star, S. L. (1999). The Ethnography of Infrastructure. The American Behavioral Scientist, 43, 377-391. doi: 10.1177/00027649921955326

Tagarev, N. (2019). *Education in Management of Cybersecurity* [Conference Session]. 9th International Conference on Future of Education, Florence, Italy. https://conference.pixel-online.net/FOE/files/foe/ed0009/FP/5943-BUSE4070-FP-FOE9.pdf

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?. *Computers in Human Behavior*, *84*, 375-382. https://doi-org.proxy1.library.virginia.edu/10.1016/j.chb.2018.02.019

BIBLIOGRAPHY

Bkakria. A., Yaich, R., & Arabi, W. (2022). Secure and Robust Cyber Security Threat Information Sharing. *International Symposium on Foundations and Practice of Security (FPS)* 2021, 3-18. doi: 10.1007/978-3-031-08147-7_1

Bowman, E. (2021). After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users. *NPR*. https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users

Cebula, J. J., Popeck, M. E., & Young, L. R. (2014). Taxonomy of Operational Cyber Security Risk Version 2. National Technical Reports Library, U.S. Department of Commerce. https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/ADA609863.xhtml

Chapman, G. (2019). Facebook admits storing passwords in plain text (Update). *Phys.org*. https://phys.org/news/2019-03-facebook-passwords-plain-text.html

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. *Applied Sciences,* 11 (10), 4580, pp. 30. https://doi.org/10.3390/app11104580

Gong, N. (2019). Barriers to Adopting Interoperability Standards for Cyber Threat Intelligence Sharing: An Exploratory Study. *Systems Engineering Technical Center, The MITRE Corporation*. https://doi.org/10.1007/978-3-030-01177-2_49

Joubert, S. (2018). Working in Industry vs Academia: Which is Right For You?. Northeastern University. Retrieved from https://www.northeastern.edu/graduate/blog/working-in-industry-vs-academia/

Kagita, M. K., Thilakarathne, N., Gadekallu, T. R., Maddikunta, P. K. R., & Singh, S. (2021). A Review on Cyber Crimes on the Internet of Things. *Signals and Communication Technology*, 83-98. doi: 10.1007/978-981-16-6186-0_4

Morales, J. A. (2018). Current Malware Trends. Carnegie Mellon University. https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/AD1087017.xhtml

Plakosh, D. (2015). Increasing Adoption of Secure Coding. Carnegie Mellon University. https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/AD1145865.xhtml

Sitharthan, R. & Rajesh, M. (2021). Application of machine learning (ML) and internet of things

(IoT) in healthcare to predict and tackle pandemic situation. *Distributed and Parallel Databases*. https://doi.org/10.1007/s10619-021-07358-7

Vieane, A., Funke, G., Gutzwiller, R., Mancuso, V., Sawyer, B., Wickens, C. (2016). Addressing Human Factor Gaps in Cyber Defense. Colorado State University, Fort Collins. https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/AD1021939.xhtml

Xingye, L. (2019). The big data impact and application study on the like ecosystem construction of open internet of things. *Cluster Computing*, 22, 3563-3572. doi: 10.1007/s10586-018-2206-z