Reflections on Cybersecurity: Integrating Risk Manageent, Ethics, and Technical Proficiency

Rebecca Hight

Old Dominion University

IDS 493

Dr. Sherron Gordon-Phan

December 4, 2024

Introduction

Throughout my degree program, I have developed key skills that are essential for a successful career in cybersecurity: analytical and critical thinking, technical proficiency in cybersecurity tools, and an understanding of legal and ethical considerations. My coursework has always been interdisciplinary as it draws from cybersecurity, ethics, law, and technical approaches that enable me to consider problems from different angles. This is showcased via a risk assessment report of an organization during my internship, exhibiting my ability to analyze network traffic and security incidents, and analyze the effects of the WannaCry ransomware attack. Every artifact demonstrates my technical and analytical skills, and, more importantly, it demonstrates how and where in my academic career and collaborative learning experiences I have been prepared to deal with actual cybersecurity issues. These competencies are especially important for my career because, without them, it is impossible to solve the tasks that are relevant to a cybersecurity professional in the 21st century.

Skill 1: Analytical and Critical Thinking Skills

Analytical and critical thinking skills are crucial in the cybersecurity profession as professionals are supposed to evaluate risks and threats and consider measures for preventing security threats. These skills enable cybersecurity experts to decipher complex information and identify indicators of compromise and precursors to risks. They also enable professionals to compare various responses to threats and select a proper type of action (Safitra et al., 2023). These thinking skills are interdisciplinary, derived from such practices as statistical analysis, regulation of risk, and law, and offer a broader perspective on cybersecurity. For example,

rationality assists in assessing the legal and ethical consequences of a data breach to guarantee that the responses are adequate and follow regulatory rules (AlDaajeh et al., 2022).

Using these skills in specific problems has been possible throughout my coursework and assignments. Specifically, during risk assessment and case studies, there was a need to assess risks, notice risks and their effects on the bigger picture, and suggest solutions. Considering those tasks, the degree to which critical thinking is important for the analysis of issues, definition of essential problems, and provision of relevant solutions was needed. These tasks proved that analytical and critical thinking are vital not only in cyberspace but also in general problem-solving.

Artifacts:

1. **Risk Assessment Report (SQL Database Risk Assessment)**:

While conducting a risk assessment of the City of Suffolk's SQL database, I analyzed and critically reasoned security risks within database systems. We evaluated threats, such as weak passwords and policies and unapplied security updates, and recommended solutions. This report illustrated how risk management and data protection information can be combined to detect vulnerabilities, assess potential threats, and implement effective mitigation strategies to safeguard sensitive data (Landoll, 2021).

2. **Network Traffic Analysis in CYSE 300**:

When analyzing traffic in CYSE 300, I learned the difference between normal traffic and suspicious traffic. With the help of analytics, I analyzed traffic flow and searched for any anomalies that may indicate malicious actions, such as DoS or unauthorized access. This exercise showed how data analysis requires critical thinking in order to work through enormous amounts of data to identify and prevent cyber threats (Papadogiannaki and Ioannidis, 2021).

3. **Case Study Analysis: WannaCry Ransomware Attack**:

One of the critical thinking skills applied during the WannaCry ransomware case was analyzing how the attack occurred and what factors needed to be scrutinized. I analyzed the possibility of exploits in unpatched software vulnerabilities and suggested solutions in accordance with risk management theories. The study also brought some ethical considerations having to do with the responsibility of the organizations to ensure that they have the latest patches for security. Additionally, this case study demonstrated the need to use critical thinking in analyzing the primary causes of vulnerabilities and identifying the right strategies for strengthening cybersecurity postures.

Skill 2: Technical Proficiency in Cybersecurity Tools

Cybersecurity tools are essential to identify security weaknesses, optimize the structure to counteract threats and incorporate technical advancements to do tasks mechanically. Software solutions such as risk analyzers, network analyzers, and log management solutions enable cybersecurity professionals to avoid threats, provide real-time views of the systems, and perform automated routine functions. For example, on the Tenable.io platform, there is always a way of identifying the weaknesses in a system and its accompanying risks, and with regard to Wireshark, it provides professionals with tools to decode and understand the flow of traffic, enabling them to notice disparate activities (Awoniyi and Kazmi, 2021). Using information from assignments and lectures, identify and discuss other factors that one needs to consider when using the tools in cybersecurity, ethical and legal considerations, and privacy regulations. Pursuing my academic education alongside applying for an internship helped me acquire relevant skills in how different cybersecurity tools work. Starting from risk assessments with Tenable.io up to network traffic analysis with Wireshark, I was shown how those tools can be aligned with

other cybersecurity processes. These experiences were a good indication of how automation and real-time monitoring can enhance system security and the responses made to threats.

Artifacts:

1. **Tenable.io Risk Assessment Tool**:

During the course of my internship, I used Tenable.io to evaluate vulnerabilities in internal systems. This tool gave me an insight into how to sort out risks according to impacts, offering me a full view of that organization's security. This placed me in a position to apply lessons learned on risk management and security of networks, touching on the fact that risks need to be detected earlier (Haybyrne, 2023).

2. **Wireshark Usage in Labs**:

During several lab assignments, I employed the Wireshark tool for traffic analysis and log files to identify security incidents. It also enabled me to have a real-time view of the activity to look for the signs of anomalies, view the source of some forms of potential intrusions, and analyze the patterns of the network for malicious activity. One particular lab exercise proved how more tools under network analysis help in security monitoring and incident handling.

3. **Python Coding for Cybersecurity Tasks**:

In a recent project, I used IDLE to create a client-server communication system, allowing two entities to exchange messages over a network. This project demonstrated my ability to implement networking protocols and manage secure data transmission, showcasing my understanding of fundamental cybersecurity concepts and technical proficiency in cybersecurity tools through hands-on experience with Python coding and socket programming.

Skill 3: Knowledge of Legal and Ethical Considerations in Cybersecurity

Awareness of legal and ethical issues is vital to cybersecurity professionals since they need to protect data from unauthorized access while at the same time following regulations such as GDPR or CCPA. These laws regulate the manner in which individuals' data is processed, and anyone who violates the laws faces legal and reputational consequences. Cybersecurity professionals are not just analysts who perform computational tasks, they also need to comprehend their responsibilities based on ethics and/or law. When confronted with probable threats to the security of a system, cybersecurity professionals must define the extent to which the system needs protection and how this will infringe on the privacy of an individual (Allahrakha, 2023). The ethical issue regarding cybersecurity can be full of conflict of interest because user privacy can be sacrificed for the sake of system security.

At the intersection of law, ethics, and technology, interdisciplinary learning is key. In the course of my learning, I came across cases where I had to apply my understanding of law and ethics alongside technical knowledge of cybersecurity. My course in cybersecurity ethics provided me with the existing legal structures, while the ethics side of the course gave me frameworks to adopt in decision-making that promote both privacy and security. This knowledge was crucial for the ethical issues that emerge in cybersecurity practices and to observe the legal boundaries to protect the users' rights.

Artifacts:

1. **Case Analysis on Legal Frameworks and Regulations**:

In the case study related to GDPR and data protection laws, I learned about the legal requirements of cybersecurity experts. This assignment allowed me to associate technical cybersecurity awareness with the necessity of compliance. I read regulations and knew how to

incorporate them as security practices to protect the systems while at the same time implementing laws such as GDPR and CCPA (Fakeyede et al., 2023).

2. **Case Analysis on Information Warfare:**

In my case analysis on information warfare, I examined ethical issues surrounding Facebook's role in the 2016 U.S. presidential election, particularly its involvement in spreading misinformation. I applied consequentialism, a moral theory that evaluates actions based on their outcomes. I analyzed how Facebook's algorithms were designed to optimize engagement that allowed fake news to spread, influencing voter behavior and ultimately contributing to the distortion of democratic processes. I used the work of Prier and Scott who highlight ethical risks posed by networked devices and social media's manipulation. This case analysis showcases my understanding of legal and ethical considerations in cybersecurity, the ethical responsibilities of digital platforms, and the broader impacts of technology on society.

3. **Case Analysis of Ethical Implications of Cybersecurity Technologies**:

In my case analysis on professional ethics using ethics of care moral reasoning, I examined the ethical dilemma faced by a software engineer who developed a deceptive quiz for a pharmaceutical company that misled users into thinking they needed a harmful drug. I applied the ethical frameworks of IEEE, ACM, and NSPE Code of Ethics to assess the engineer's decisions and actions. This highlighted the importance of professional responsibility in cybersecurity and the welfare of users in all technology-related decisions. I applied the legal and ethical concepts to a real-world scenario, demonstrating my understanding of the ethical challenges cybersecurity professionals may face in their careers.

Conclusion

The analytical thinking skills, technical skills, and legal and ethical understandings mentioned in this reflection make me ready for my career in cybersecurity. These skills enable me to solve problems by having a broad view of the problem and other considerations to make while applying technical know-how and legal and ethical aspects of a problem. The interdisciplinarity of the courses I have taken has been useful in instilling in me how the different disciplines address cybersecurity challenges. This wide, cross-sectional perspective will be crucial and influential when operating in the constantly evolving cybersecurity industry to provide proper and lawful conclusions in my future career.

References

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K.K.R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security, 119*, 102754. https://doi.org/10.1016/j.cose.2022.102754

Allahrakha, N. (2023). Balancing cybersecurity and privacy: Legal and ethical considerations in the digital age. *Legal Issues in the Digital Age, 2*, 78-121.

Awoniyi, S., & Kazmi, M.A.N. (2021). Determining vulnerabilities of pervasive IoT devices and their geographic distribution. In *Challenges in the IoT and Smart Environments: A Practitioners' Guide to Security, Ethics, and Criminal Threats* (pp. 211-243). Cham: Springer International Publishing.

Fakeyede, O.O.O., Okeleke, P.A., Hassan, A.O., Iwuanyanwu, U., & Adaramodu, O.R. (2023). Navigating data privacy through IT audits: GDPR, CCPA, and beyond. *International Journal of Research in Engineering and Science, 11*(11).

Haybyrne, M. (2023). An investigation into the benefits of risk management & monitoring to aid cybersecurity in an SME (Doctoral dissertation, National College of Ireland).

Landoll, D. (2021). *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC Press.

Papadogiannaki, E., & Ioannidis, S. (2021). A survey on encrypted network traffic analysis applications, techniques, and countermeasures. *ACM Computing Surveys (CSUR), 54*(6), 1-35.

Safitra, M.F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability, 15*(18), 13369. https://doi.org/10.3390/su151813369