

Alek Norris

Jeff Franklin

CYB E 234

03 MAY 2024

## Final Essay

As I've progressed through my Cybersecurity ethics course this semester, I've gained a deeper understanding of my ethical values and the Cybersecurity field. In this essay, I'll reflect on the lessons and knowledge gained, exploring the ethical principles that guide professional conduct in the industry, including integrity, confidentiality, accountability, privacy, legality, professional development, and public interest. I'll also assess how this course has impacted my personal evolution by comparing my ethical values before and after. In subsequent sections, I'll discuss my current soft skills, how to improve them, and how I'll incorporate these ethical standards into my future endeavors. Additionally, I'll identify the most challenging areas for me and how I plan to cope and strategize to remain accountable.

Discussing the key factors that guide my ethical compass is essential. Some of these factors were ingrained in me before this course, while others were acquired during it. Nevertheless, each holds equal importance. This is because there is never a clear-cut right or wrong answer, and having a diverse range of considerations to bear in mind will always steer me in the right direction.

Integrity is the first and most crucial factor. It involves upholding honesty and strong moral principles. This is vital in our field of work as it guarantees we deliver on our promises. For us, that may entail performing checks, filling out paperwork, and patching a system. For our

clients, this translates into safeguarding their data, creating a paper trail, and fulfilling our contractual obligations with utmost diligence.

Similar to integrity, we have confidentiality. Confidentiality means that we are protecting our client's information, but not necessarily in the most outlined routes. Confidentiality means anything we see, hear, or read, intentionally or not, must stay in our brains, and we ensure that only those who are intended to see information get that information. It's similar to keeping a secret in some way.

Next, we have accountability. Accountability is crucial in the cybersecurity field, as it is in any other profession. It means taking responsibility for my actions, owning up to mistakes, and ensuring that I complete my work thoroughly and efficiently. I don't wait for others to remind me of my responsibilities but seek to fulfill them proactively. As a cybersecurity professional, I also greatly value respecting individuals' privacy rights. This means that even if I have access to sensitive information, I do not abuse that privilege and only access what is necessary for my work. I may even establish guidelines to ensure compliance with privacy laws and regulations., Which leads us to legality.

Legal compliance is a crucial aspect of our work that we must always uphold. The high-pressure environment of the cybersecurity field can sometimes cloud our judgment and make us forget that our actions may not always be legal, even if we can access information in any way we see fit. We must know what is legally permissible and what is not and ensure that all our actions are well-documented. Failure to do so could have severe and far-reaching consequences, even if we did not intend any harm.

In navigating these legal complexities, I believe it is essential to understand that today's ethical decisions help shape tomorrow's cybersecurity norms. Many places currently have poor

ethical frameworks in which they work, especially regarding legalities. It is essential to know that Each choice to uphold or bypass legal guidelines impacts our immediate projects and sets precedents that influence industry standards. Someone somewhere must always start a trend, and by committing to strict legal compliance, we protect our organizations from legal repercussions and contribute to developing a robust ethical culture in cybersecurity. This commitment ensures that we remain vigilant guardians of not only data but also the trust placed in us by users and stakeholders, reinforcing the integral role of ethics in our professional lives,

In addition to legal compliance, we must consider the public interest. As cybersecurity professionals, our actions can significantly impact our companies and the public. We must be mindful of this responsibility when making decisions such as skipping a software patch or neglecting SIEM alarms. A data breach can result in millions of dollars in losses for a company, as seen in the Target breach of the last decade. Our actions behind the scenes can directly affect how the public views our employers, so we must always keep that in mind and strive to do our best at all times.

Lastly, it is crucial to prioritize professional development by continuously updating our skills and being proactive learners. This goes beyond simply learning a new coding language or security practice. As the field is dynamic and constantly evolving, taking the initiative to stay up-to-date on technical and ethical practices is essential. By being on the lookout for learning opportunities, we can further develop our abilities and decision-making skills.

Before taking this class, I recognized the importance of the values mentioned above to varying degrees but did not fully grasp their significance. My understanding of integrity, confidentiality, accountability, and professional development was limited. I had not given much thought to concepts such as respect for privacy, legality, and public interest.

When I first learned about integrity, confidentiality, accountability, and professional development, I understood what each word meant. For instance, I knew that integrity involved keeping promises. But as I've delved deeper into my field, I've come to see how each of these concepts plays out in practice. For instance, I now understand that integrity also involves going above and beyond to ensure that updates are completed on time and that potential issues are addressed proactively. Similarly, while I was familiar with the definitions of confidentiality and accountability, I now appreciate the importance of applying these principles to protect both our customers' legal rights and trust. Maintaining confidentiality is critical, and we must always be vigilant for any signs of potential breaches.

Being in the military, I had always seen accountability as being sure to follow through with what I say, be where I need to be, and take responsibility for my actions. After finishing this class, however, I now see that it extends beyond taking care of myself. In cybersecurity, this means being accountable for everything I touch or work with, taking pride in everything I do, getting things done promptly, and making sure we hold those around us to a standard and help them where they need it. It also means keeping up with the CVEs, the paperwork, the boring, mundane stuff, and ensuring we are always doing everything to our standard and the company's required standard, which is where professional development comes in.

My original view on professional development was mainly about continuing to grow my skills and knowledge in the I.T. realm. This meant learning troubleshooting, debugging, languages, patterns, etc. However, since taking this course, I have realized that it means that and so much more. Professional development in this field means always being on the lookout for new issues, CVE patches, vulnerabilities, and updates to laws and regulations. It also means

explaining my work and articulating my words in ways so that non-technical users can understand the importance of the aspects they need to know.

The three newer factors for me are respect for privacy, legality, and public interest. These three were known to me but were not high on my list initially. For respect for privacy, I just saw it as not meddling with others' data or viewing where I don't need to. However, during this course, I realized it also means being conscious of the laws and regulations, such as the General Data Protection Regulation in Europe or the National Institute of Standards and Technology, specifically 800-53. Both have extensive information on frameworks for privacy and how data can and cannot be handled when it comes to working in this field. Because of this realization, I have concluded that my small understanding of respect for privacy may not be how others or the law sees it.

Previously, I used to conflate public interest with privacy. I believed that in any job I took, the only public interest I needed to consider was that of those around me, my superiors, or my employer. By prioritizing this, I could avoid accidentally revealing personal information and, in turn, avoid any negative repercussions from the public. However, after completing this course, I now understand that public interest encompasses much more than privacy. It involves being mindful of the effects of our work on society and always prioritizing the well-being of the public, even if it means putting aside personal gain or interest.

Let us now examine the legal aspect, which is a critical consideration. In the past, legality was often viewed as a simple matter of asking if something was legal and moving on. However, I now understand that this is a limited perspective. The legal implications of our actions can significantly impact our professional lives, determining whether we succeed or face

imprisonment. Moreover, legal boundaries can influence whether we are charged with a crime or viewed as having malicious intent while merely performing our duties. A case we discussed in class concerning pen testing comes to mind. Two employees were hired to conduct pen tests at a courthouse, but they were subsequently arrested and faced prosecution. Ultimately, the person who hired them lacked the authority to permit their actions. As a result of this oversight, their employer and the client were compelled to pay a steep price in terms of time and money. Although the charges were eventually dropped, this instance underscores the importance of paying attention to legal matters.

It is vital to recognize that blindly following instructions can have negative consequences, both ethically and legally. Therefore, it is advisable to double-check everything you do to ensure that it complies with ethical rules and governing regulations. Neglecting to do so could lead to a significant setback in your career.

Apart from these factors, one should regard other soft skills as equally important. Soft skills, while often not quantifiable on paper, can directly impact one's success. In the realm of cybersecurity, I have learned about three soft skills in this class that I believe are essential to guiding my ethical compass: critical thinking, adaptability, and ethical judgment.

On this list, the ability to think critically is of utmost importance. It encompasses the capacity to assess one's position and devise a practical solution for the given task. This necessitates a comprehensive grasp of one's starting point, destination, and steps to bridge the gap. In the realm of cybersecurity, there are no one-size-fits-all solutions, requiring adaptability in every situation. Whether it involves troubleshooting a problem, conducting a pen test, or deciding whether to follow superiors blindly, the ability to adjust to changing circumstances is critical.

This implies that in the cybersecurity field, individuals must not only be proficient in computer skills but also be able to distinguish between right and wrong. If an action is incorrect, is it due to personal morality or legal implications? This skill may differentiate between a job well done, working late, or losing one's employment entirely.

In cybersecurity, adaptability is a crucial skill that requires a great deal of critical thinking. It involves thinking on your feet and adjusting to the current situation, which may require stepping outside of your comfort zone, changing your team, or responding quickly to shifting environments and new systems. With computers advancing rapidly, even if we possess a comprehensive understanding of everything today, we may fall behind on trends within a few years. Thus, the ability to adapt is paramount in this field.

In addition, ethical judgment is a fundamental aspect of cybersecurity. It involves distinguishing right from wrong in complex situations and making decisions that adhere to legal and ethical standards. This skill is developed through a deep comprehension of ethical principles and their practical applications in cybersecurity. Cybersecurity professionals cannot be trusted to handle sensitive data without sound moral judgment. They must be able to discern right from wrong both on a professional and personal ethical standard level. They must treat data with the utmost care at work and at home.

Maintaining soft skills and other factors can prove to be challenging. Personally, I find ethical judgment, critical thinking, and professional development to be the most difficult. These areas require significant time and commitment to master, and it can be hard to avoid burnout.

Ethical judgment can be a blurry line, depending on the situation. It may seem right in some aspects but utterly wrong in others, such as someone's personal beliefs. For instance, the NSA created the SMB Eternal Blue exploit for national security purposes. While it's essential to

be proactive in national security, accessing anyone's computer without their knowledge or consent doesn't seem ethical. In such cases, difficult decisions must be made, and a clear-cut answer may not exist. To address this, it's essential to take courses like this to understand oneself better and develop a solid moral compass.

However, maintaining momentum in critical thinking and professional development can present another set of challenges. Dedication to one's work field is necessary for success. This includes taking required ethical courses in college, ensuring technical skills are current, and prioritizing rest for the next day. Trying to keep up with everything required in the field can lead to burnout, which can have a ripple effect. To prevent this, mindfulness, meditation, or physical activity can help manage stress and establish a work-life balance. There are many ways to avoid burnout, and individuals should find what works best for them.

Upon reflection, my journey through cybersecurity ethics has deepened my understanding of the fundamental principles that govern this field and has contributed to shaping my ethical framework. The principles of integrity, confidentiality, accountability, privacy, legality, professional development, and public interest are all crucial components that must be upheld to maintain trust in our increasingly digital world. I am confident that the knowledge and insights I have gained from this course will guide my actions and decisions as a cybersecurity professional, ensuring that I always strive to uphold the highest ethical standards and make positive contributions to the field.

As I review the evolution of my understanding and the reevaluation of my ethical values, it is clear that this course has been truly transformative. The practical application of these ethical principles in real-world scenarios has equipped me with the tools and perspectives necessary to approach challenges with balance and fairness. Moving forward, I am better prepared to handle



sensitive information with the utmost respect for privacy and legality and to continue my professional development in this dynamic field. My ongoing commitment to ethical excellence, accountability, and continuous learning will benefit my career and contribute to the broader goal of creating a secure and ethical digital environment.

## Works Cited

Because of the contents requested in this final essay, such as personal learning and reflection on in-class discussions, I have not directly quoted anything I feel should be mentioned here as it was all something talked about in class at least once, or it was a personal opinion.

## Acknowledgments

I want to acknowledge using Grammarly A.I. for grammar and style enhancements in preparing  
this document.