Carlos Carey

Professor Armistead

Journal Entries

01 February 2023

Journal Entry #1 01-14-23

Question: **Review the NICE Workforce Framework. Are there certain areas that you would want to focus your career on? Explain which areas would appeal the most to you and which would appeal the least.**

Even though I am currently going through the process of transferring colleges, and changing majors (automotive trades through TCC) there are some fields I was interested in before my current revelation. I was interested in things that fall under the operation and maintenance category, such as network services or systems administration. These jobs would be ideal for me because of the minimal human interaction needed. Not only is minimal interaction needed, but I can also do my job peacefully without being bothered as long as I do my job correctly and maintain security.

For those career fields one finds interesting, there are ones that someone doesn't want to do. Mostly anything that falls under the oversee and govern section is something that I wouldn't want to do. My social anxiety prevents me from doing something so prestigious and being a leader. This is why anything that involves leading or guiding others wouldn't suit me, which is why anything that falls under the oversee and govern section would not be anything I'd specialize in.

Journal Entry #2 01-20-23

Question: **Explain how the principles of science relate to cybersecurity.**

The principle of Relativism is in the name, as it states that all things are related. This is hard with cybersecurity due to the consistent development of new technologies within the field of cybersecurity along with the field branching out. This affects people daily for better or for worse.

Objectivity says that things should be handled indifferently. An example of this is how we handle children/teens committing crimes online vs adults, objectivism states that regardless of the differences, the punishment should still be the same.

Parsimony is all about the simplicity of explanations. It is meant to help people who don't fully understand the field of study by it being simplistic and easy to understand. We all know hackers hack for financial gains, entertainment, or even for publicity, something parsimony could be used for. With the complexity of the brain, the motive won't be known, parsimony wouldn't help explain why hackers hack, it just acknowledges their possible reasons/motives.

Empiricism follows the ethical standards of society, as it goes with what is considered morally just and unjust. A current example of this is when a company tracks a user's activity, is it ethical for the company to do this?

Determinism states that actions take place due to actions and decisions made before, like a domino effect. In cybersecurity, if your security infrastructure is of poor quality, you are going to be hacked. Vulnerabilities will be used against you, not a matter of if, it's a matter of when with determinism. Determinism helps with foreseeing these issues and allows you to take preventive measures.

Journal Entry #3 01-28-23

Question: **Visit PrivacyRights.org to see the types of publicly available information about data breaches. How might researchers use this information to study breaches? Enter a paragraph in your journal.**

The information the website provides researchers is vital as it helps them understand what types of breaches are commonplace, how to safeguard against those breaches and train their employees as most breaches occur due to human error and faults. Having access to this information allows people to become more self-aware and less likely to become a victim. This information also helps employers and large companies to learn from the mistakes of others and implement a better way to protect their information.

Journal Entry #4 02-01-23

Question: **Review Maslow's Hierarchy of Needs and explain how each level relates to your experiences with technology. Give specific examples of how your digital experiences relate to each level of need.**

The first level of the hierarchy is physiological needs. They tend to relate to things people can't live without, such as food, water, air, etc. Many people have developed an attachment to technology and seem to think they can't live without it. For me it causes distress as without technology I cannot check my finances at a moment's notice, nor can I check my email. The second level is similar to safety needs. When I have hacked a while ago, I felt very powerless as they began to take money out of my account due to not having much prior knowledge of the event. Social belonging is the third level, and some people struggle with a physical feeling of belonging so they turn to the digital world. I am a car fanatic, and in my free time I work on cars, not many people at ODU are, so I turn to the digital world to find like-minded people who do similar things to bond with. Esteem is the fourth level and can be put into two categories, one is peer acceptance and self-acceptance. Some people turn to technology for support which can have positive and negative outcomes. The fifth level and most broad is self-actualization. This is when one feels indifferent to other people's opinions and is granted a level of self-accomplishment and when one feels they are to their full potential.

Journal Entry #5 02-11-23

Question: **Cyber Crime Isn't about Computers: It's about Behavior" by Adam Anderson, think about how individuals' beliefs place them at risk for cyber-victimization. How does fishing relate to cyber victimization? How does a doctor washing their hands relate to cybersecurity?**

Individuals may be more susceptible to phishing scams in connection to cyber victimization depending on their beliefs. People may be more likely to click on links or give personal information without first checking the request's legitimacy if they believe they can trust any email or message that appears to be from a reputable company, such as a bank or social media platform. This could enhance their vulnerability to phishing assaults and the risk of online exploitation.

Using the example of a doctor washing their hands, we may compare cybersecurity to proper cyber hygiene. To defend oneself from cyber risks, people need to adopt appropriate cybersecurity practices as part of their regular behavior, just as doctors wash their hands frequently to prevent the spread of illnesses. This may entail frequently changing passwords, exercising caution when clicking on dubious links or downloading attachments from unfamiliar sources, maintaining software and operating systems with the most recent security patches, and being aware of social engineering tactics used in cyberattacks.

Journal Entry #6 02-18-23

Question: **Can you spot three fake websites and compare the three fake websites to three real websites, plus showcase what makes the fake websites fake?**

For example, www.paypal-supports.com has a different domain name which then leads you to a different website when you wanted to go to www.paypal.com. This website may end up requesting information in a sketchy manner. Another example of this is www.bankofamerlca.com where they replaced the "i" in America with an "l". This will then lead you to a knockoff of the Bank of America that requests banking information masquerading as the actual bank. A final example would be www.lcloud.com which ends up looking just like the official Apple www.icloud.com and asks for information in almost the same way.

Journal Entry #7 02-25-23

Question: **Review the ten photos and create memes through the perspective of the cybersecurity human systems integration framework.**

Photo 1: The meme could portray the person's mind as split between cybersecurity best practices and risky behaviors, with conflicting thoughts on how to protect their online activities.

Photo 2: The meme could depict the person's mind as focused and vigilant, actively considering potential cyber threats and taking necessary precautions.

Photo 3: The meme could illustrate the person's mind as struggling to understand the complexities of cybersecurity and how to safeguard their mobile device and personal information.

Photo 4: The meme could convey the person's mind as being caught off guard by a cyber attack, highlighting the need for constant awareness and preparedness.

Photo 5: The meme could portray the person's mind as being overly complacent about cybersecurity, neglecting important security measures, and leaving themselves vulnerable to potential threats.

Photo 6: The meme could depict the person's mind as actively considering the risks and benefits of different online activities, and making informed decisions to protect their digital assets.

Photo 7: The meme could illustrate the person's mind as struggling to understand complex cybersecurity concepts and seeking guidance on best practices.

Photo 8: The meme could portray the user's mind as a blank slate, lacking awareness and knowledge about cybersecurity, and the need to educate oneself on safe online practices.

Photo 9:The meme could depict the importance of incorporating cybersecurity education and training into various learning environments, including schools and educational programs.

Photo 10: The meme could highlight the prevalent use of mobile devices in our daily lives and the need to prioritize cybersecurity measures, such as using strong passwords and keeping devices updated.

These memes highlight the value of Human Systems Integration (HSI) in promoting secure online behavior, education, and training for people within the larger cyber ecosystem by illustrating how different levels of awareness, knowledge, and behaviors related to cybersecurity may be reflected in the minds of the individuals in each meme.

Journal Entry #8 03-03-23

Question: **Watch this video and pay attention to the way that movies distort hackers.**

Hacker Rates 12 Hacking Scenes In Movies And TV | How Real Is It? - YouTube

After watching, write a journal entry about how you think the media influences our understanding of cybersecurity.

I now think that the media has a big impact on how we perceive cybersecurity, having watched the film. A glorification of hacking has resulted from the frequent portrayal of hackers as persons who can easily break into any system, steal data, and influence systems. People may feel that cybersecurity is simple to handle and that hackers are superhumans as a result of this representation, which can lead to misunderstandings and irrational expectations.

Additionally, a lack of knowledge of the dangers posed by technology may be caused by how cybersecurity is portrayed in the media. To secure themselves and their data, people must take the necessary precautions as cybersecurity dangers rise as technology becomes more pervasive in our everyday lives. The media's presentation of cybersecurity, however, can give people a false feeling of security, making them think they are not in danger or that they are not in charge of protecting their digital assets. As a result, people may get complacent and reject recommended procedures for cybersecurity, leaving them more open to cyberattacks.

Journal Entry #9 03-10-23

Question: **Complete the Social Media Disorder scale. How did you score? What do you think about the items on the scale? Why do you think that different patterns are found across the world?**

Due to diverse cultural, socioeconomic, and individual factors, different social media usage trends and their effects may be observed around the world. Social expectations, technology infrastructure, and cultural norms and values may all affect how people use social media. Social media, for instance, maybe more ubiquitous and generally acceptable as a form of communication in some cultures while being less so or even frowned upon in others.

Individual variations including personality traits, age, and personal preferences can also influence how someone uses social media. While some people may view social media as a useful tool for networking, self-expression, and socializing, others may see it as having negative effects including addiction, diminished well-being, and social isolation.

Journal Entry #10 03-17-23

Question: **Read this and write a journal entry summarizing your response to the article on social cybersecurity**

https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Mar-Apr-2019/117-Cybersecurity/b/

In order to defend against online attacks, the paper underlines the value of social cybersecurity. It argues why social engineering assaults, which take advantage of psychological flaws in people to access sensitive data or systems, pose a serious risk to cybersecurity. The essay also emphasizes the significance of social and behavioral elements in risk assessments and security plans for cybersecurity experts.

The paper raises several crucial issues about the part played by social variables in cybersecurity. It emphasizes the fact that technology solutions alone are insufficient for successful cybersecurity and that social engineering assaults may be just as harmful as technical flaws. The article can assist people and organizations in better defending themselves against online attacks by bringing these concerns to people's attention.

Overall, the essay offers insightful information on the significance of social cybersecurity and the demand for an all-encompassing strategy for cybersecurity that takes into account both technological and social issues. It serves as a reminder that cybersecurity is not simply a technological issue, but also a social and behavioral one, and that successful cybersecurity plans must take both facets into account.

Journal Entry #11 03-18-23

Question: **Watch this video. As you watch the video https://www.youtube.com/watch?v=iYtmuHbhmS0, think about how the description of the cybersecurity analyst job relates to social behaviors. Write a paragraph describing social themes that arise in the presentation.**

The speaker in the video discusses the function of a cybersecurity analyst and how it connects to social behavior. The necessity of communication skills in the world of cybersecurity is one of the social topics that emerge in the presentation. The speaker stresses the need for excellent communication skills for cybersecurity professionals with both technical and non-technical coworkers who may come from diverse backgrounds or areas of expertise. The value of cooperation and teamwork in the sphere of cybersecurity also stands up as a major subject. The speaker discusses how teams are common among cybersecurity experts, and how these teams need to be able to collaborate well to detect and neutralize threats. Finally, the speaker highlights how critical thinking and problem-solving abilities are crucial in the subject of cybersecurity. She explains how cybersecurity analysts need to be able to deconstruct difficult issues and generate novel solutions to defend their businesses from online attacks.

Journal Entry #12 03-25-23

Question: **A later module addresses cybersecurity policy through a social science framework. At this point, attention can be drawn to one type of policy, known as bug bounty policies. These policies pay individuals for identifying vulnerabilities in a company's cyber infrastructure. To identify the vulnerabilities, ethical hackers are invited to try to explore the cyberinfrastructure using their penetration testing skills. The policies**

related to economics in that are based on cost/benefits principles. Read this article https://academic.oup.com/cybersecurity/article/7/1/tyab007/6168453?login=true and write a summary reaction to the use of the policies in your journal. Focus primarily on the literature review and the discussion of the findings.

After reading the article on cybersecurity bug bounty programs, I find the idea fascinating and believe it could improve cybersecurity defenses. The examination of the literature offers a thorough overview of bug bounty programs and how they have changed over time, emphasizing how more businesses are adopting these programs as a proactive means of detecting weaknesses in their cyberinfrastructure.

The analysis of the data shows that bug bounty programs have had encouraging outcomes in terms of identifying vulnerabilities and boosting cybersecurity posture. Participating in bug bounty programs allows ethical hackers, often known as "white hat" hackers, to use their knowledge to find security flaws that could be missed by conventional security procedures. The essay also covers the financial side of bug bounty programs because they are based on cost-benefit analysis and reward ethical hackers in return for finding vulnerabilities. This strategy encourages ethical hackers to actively look for weaknesses and notify enterprises of them, which may lead to more secure cyber infrastructures in the long run.

I value the perspectives the essay offers on the advantages and difficulties of bug bounty programs. It emphasizes the necessity for businesses to properly plan and manage bug bounty programs, taking into account things like financial incentives, the breadth of testing, and any potential legal repercussions. The article also highlights the restrictions of bug bounty programs, including potential legal and ethical issues, as well as the dependence on the skills and expertise of ethical hackers.

In conclusion, bug bounty policies can be a valuable approach to improving cybersecurity by harnessing the skills of ethical hackers to identify vulnerabilities. However, they also come with challenges that need to be carefully considered and addressed. The article provides a comprehensive overview of the literature and findings related to bug bounty policies, offering valuable insights for policymakers, organizations, and ethical hackers alike.

Journal Entry #13 04-04-23

Question: **Andriy Slynchuk has described eleven things Internet users do that may be illegal. Review what the author says and write a paragraph describing the five most serious violations and why you think those offenses are serious.**

Eleven criminal behaviors that internet users could participate in online are highlighted in the essay by Andriy Slynchuk. Five of them are the most severe offenses:

1. Using a 3rd party streaming service watching the newest tv show without paying for the actual service is an illegal thing millions of people do every day.
2. When people put together presentations they unknowingly use images that may be copyrighted and then can get into legal trouble for not having permission to use the image.

3. Posting someone's address online because you got mad and hacked them to get

their IP. Yes, this is very much illegal but people do it on a daily as a way to express their anger with someone.

4. Yes, Cyberbullying is considered a crime. I don’t personally think this should be considered a crime because all you have to do is turn it off or log out, however, it’s still considered criminal.

5. Online fraud is It is a significant offense to engage in fraudulent acts online, such as phishing, scamming, or misleading others for financial gain. Cybercrime can devastate people's financial well-being and undermine their trust in online interactions and transactions. It can also cost governments, businesses, and organizations a lot of money.

These crimes are regarded as serious because they include illegal activities that have the potential to harm people, organizations, and society at large. They frequently have negative financial, legal, and reputational repercussions for the perpetrators as well as potentially lifelong effects on the victims. It is crucial for internet users to be aware of the legal ramifications of their online behavior and to utilize the internet ethically and legally.