Journal Entries - Jonathan Roeseler

Forensics pathway - journal entry 15

His journey is very unique, as digital forensics was fairly new, and only a few places offered courses on it - so he grew into it. From an accountant to a digital forensics job is interesting, but all it took was a motivated person who somewhat knew their way around a computer. I think the accountant job helped him tremendously, as an accountant, understanding integrity, as well as a chain of custody(where something comes from), is needed to perform the job well. He wrapped up the speech beautifully, reinforcing that a digital forensics investigator does not necessarily need to come from an IT background - although that would help if looking at a digital forensics investigator career.

Illegal use - Journal Entry 14

Using unofficial streaming services heavily impacts the economy, it keeps many studios from being able to produce more content or even make ends meet. Another serious violation is recording a VoIP call without consent - this activity may be used for funny purposes, but it can do much harm. Another serious violation is bullying - this can heavily impact the person receiving the unjust treatment- in some cases leading to suicide. Faking your identity can also jeopardize the wrong person, so users should avoid identifying as another person, even if it is a joke. Finally, using other's network without permission is illegal - as stated in the article it is essentially stealing, as they are paying for your network use.

Bug Bounty Programs - Journal Entry 13

The use of bug bounty programs is an effective way for organizations to identify vulnerabilities, even those with less of a budget. Despite the lower payment abilities of these organizations, these companies are still heavily investigated by hopeful researchers and/or those looking to score a bounty. The study results prove many researchers are not just in the field for money, but for proving themselves, having a good time, and finding potentially unique vulnerabilities. The study also demonstrates that by expanding the attack vector (giving bounty researchers more domains and code to "attack") an organization can ensure they are getting the best results from crowdsourced security research.

Data Breach - Journal Entry 12

Laisssez-fare relates to the letter as a relaxed approach to cybersecurity from any organization with access to your information is a major threat. Organizations should be encouraged and forced to comply with measures protecting your information. Furthermore, it

shows Keynesian economics through some government intervention - in this case involving law enforcement investigating the matter as well. A social scene theory that immediately reveals itself is the social contract - in which the organization devolved some of its authority and freedom to law enforcement in exchange for protection and security.

Cyber analyst > social themes - journal entry 11

A cyber analyst is the first line of defense for a network. Therefore most of the time a cyber analyst will find themselves responding to a phishing attack, as described in the video. Phishing attacks are the most common type of attack, as they are geared at deceiving people, not necessarily systems, as people are much easier to trick and exploit. Social engineering is another big attack that cyber analysts must properly prepare for by training users to look out for it and putting up proper systems in place to reduce the likelihood of a successful attack – a good example would be setting up an email security system like Mimecast(which prevents and blocks most phishing attacks).

Social cybersecurity - journal entry 10

The article demonstrates that the world is at risk due to how fast information can now spread over social networks. This information poses a risk to society, nations, and governments if left unchecked. As described in the article, states use social media to their advantage to create/start false narratives to weaken a country's values and military. Social science researchers on both sides- offense and defense, find ways to exploit social networks or prevent misinformation campaigns. Their research is based on human behavior and reactions, leveraging tools like machine learning to speed up their theories and research. Ultimately, it is necessary to educate citizens/users about the risks online and how they are potentially being exploited for an enemy nation’s gain.

Social Media - journal entry 9

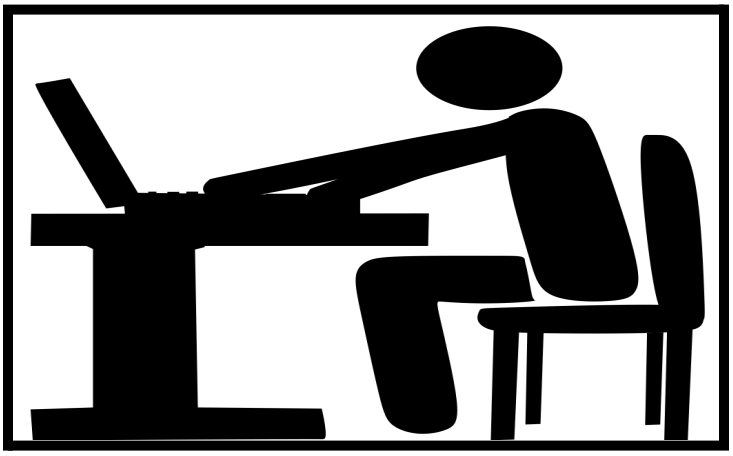
Only one of the categories applied to me (trying to reduce a lot of my social media use- I have done so only a little). I think many teens growing up today have experienced a social media disorder sometime in their lives because of how prevalent phones and social media are. Many people grow up with their phones and thus are usually attached to social media and spend a lot of

time on it to reduce stress and/or talk or communicate with their friends and family. Different patterns are found around the world as cultures emphasize different values, for example maybe a culture respects nature more than another; and therefore, its population is not as tied to their phones and social media. Another good example is maybe a specific culture only values phones for emergencies or uses them to communicate (via a phone call) with their friends.

Media Influence on Cybersecurity - journal entry 8

The movies like to portray hackers as having superhuman intelligence, which is not the case. Many of the most popular and common attacks can be done by almost anyone, so long as they have an electronic device and a connection. For example, many hacks occur over someone claiming to be someone they are not (social engineering) or as simple as a person clicking on a link in an email (phishing). Additionally, sophisticated attacks will always take more than one person to carry out - the amount of knowledge needed to reverse engineer a polymorphic malware or hack a system to save the world takes a lot of well-trained “hackers”.

Human-Centered Cybersecurity - journal entry 7



When you just remembered your password but it is incorrect

- What's on their mind? I swear this is the right password, let me try it again.

When one of your co-workers clicks on a phishing link from an outside company that conducts the tests

- What's on their mind? Why do I have to be here because someone clicked on a link? This is a waste of time.

Job searching because you got fired because of your employees clicking on every link in an email

- What's on their mind? Why am I at fault and the scapegoat for my employee's mistakes?

Fake Websites - journal entry 6

Many times, fake websites impersonate shipping companies. It is easy to tell if it is legit or not for various reasons. Attached below is an example from UPS's examples of fraudulent websites. (Note: there are three more examples here: https://www.ups.com/assets/resources/webcontent/en_US/fraud_web_examples.pdf)

One of the first things that sticks out and happens on a lot of these scam sites, is the wrong language, For example, if it were legit, the language should correspond to where you are based, not default to a different language. Additionally, if you were to look at the link, you'd see it is nowhere close to being an official UPS site(http://www.fsdhl.com.cn/ups/ups-lx.htm). Finally, another easy way to tell is if you click back or click on another tab on many of these sites, the pages don't work, they are just there for the show to entice the victim to enter PII (Not recommended to click on further tabs if you do end up on a malicious site however).

Cybercrime Motivations - journal entry 5

1. Multiple Reasons
2. Political
3. Money
4. Revenge
5. Entertainment
6. Boredom
7. Recognition

I put multiple reasons at the top of my list for making the most sense for cybercrimes because many hackers do have various reasons for hacking a company or organization – whether it be because they are bored and feel a company is malicious or even for political reasons and they are just getting paid to do it. I put political second, as many hackers are backed by their country or expose the data of an organization's wrongdoing. I put money third as both white and black hat hackers get paid a lot for what they do. Fourth is revenge- a little more rare, however, there have been many devastating attacks because of a disgruntled/fired employee or a company just messed with the wrong person. Entertainment and boredom are somewhat similar, but it is still a solid motivation, as those with a lot of time want something to do. Finally, recognition, in my opinion, is the least motivational for hackers, I have not seen it as often as the other motivations mentioned.

Maslow's Hierarchy of Needs - journal entry 4

Technology connects with many of my basic needs, especially in college. For example, it fulfills my physiological needs as I need my phone to order food and sometimes even rest as I use it to play music to fall asleep. Additionally, my phone helps me feel more secure, without it I feel like I have an empty voice in the event of an emergency. The Belonglieness level also relates to my experience with technology as it is the easiest and most effective way to communicate with close friends/partners. Furthermore, technology can impact my esteem, for example, seeing others succeed when you are feeling down can hurt. Finally, the self-actualization level. Technology has always been a hobby of mine, and working with it is my career choice, which is where I hope to find and explore my potential. Additionally, I spend a lot of my free time playing around with technology looking to learn something (my choice of a creative activity).

How might researchers use this information to study breaches? - journal entry 3

Publicly available information is crucial for organizations and researchers to advance the field of cybersecurity and help prevent a new wave of attacks, For example, by using this information with trend analysis, an attack can be better planned for and mitigated. Let's say financial companies have been targeted lately by a large amount of insider attacks. If a researcher can correctly identify this trend, devastating attacks can be prevented, saving numerous organizations time and money. Additionally, with the extra information provided by the site, a researcher can understand what types of attacks/breaches are more devastating than others from both a financial and reputation standpoint – again allowing a researcher to save an organization time, money, and reputation if properly mitigated.

Explain how the principles of science relate to cybersecurity. Journal Entry 2

One of the most important principles of science in cybersecurity is ethical neutrality. Ethical neutrality relates to the fact that scientists and researchers must be ethical in their processes. For example, imagine if a powerful technology such as GPT-4 was biased or used for unethical purposes – our world would be much different, and many people would suffer the consequences. Thus, researchers and scientists must remain ethical in their studies, especially regarding the digital/cyberspace we live in today. Another similar principle is objectivity. Those engaging in research should not be in it for malicious purposes, but simply to advance knowledge – which has luckily been done very well with rollouts of advanced AI systems/platforms to the public. If

cybersecurity did not adhere to objectivity, the internet would be much less safe and harder to access.

Journal Entry 1

A lot of the categories have jobs I would heavily consider pursuing a career in. However, my main career goal is to eventually be a Vulnerability Researcher or a Penetration Tester. So, Protection & Defense, Design and Development, and Oversight and Governance are most suited for my future goals. I specifically found that vulnerability analysis, software security assessment, and security control assessment are interesting jobs to have. Despite having an interest in these other work role categories, I do find them less appealing than the others. The least appealing to me are Investigation and Cyberspace Intelligence. Although both are crucial to cybersecurity, they do not offer as many opportunities for the job I want.