Dylan McCann

Career Paper

CYSE 201S

7/31/2024

The world of cybersecurity is a field that must consider pulling from multiple fields of research to achieve even the minimum of desired goals. It is important to realize that while technical roles and hard sciences are the foundation of all roles within our industry, social sciences play a crucial role in determining motivations, causes, and outcomes of significant events. It is commonly repeated within the industry that the human factor is always the most significant security risk so taking the time to implement the knowledge from fields that interact with the human element more directly is incredibly important for advancement and maintaining safe operations. I will be examining the cybersecurity role of information security analyst to see how social sciences can be used within this career path.

It is no secret that social engineering attacks are a current problem within the cyber security space, looking to take advantage of the human element of security. With attacks such as phishing attacks, dumpster diving, scareware, deepfakes, and many more it has become crucial to understand why they work and how to prevent potential bad actors from taking advantage of them. Understanding the psychology of social engineering attacks is especially utilized in the social cybersecurity area research maneuvers (Umphlet, Module 10). A study on social engineering attacks and effective counter measures, it was found that part of why social engineering attacks, like scam phishing emails, are so effective is because of the level of trust we place in the websites we use, and phishing emails will look to appeal to social influence, one example of influence they use is value influence and such as how a person may be persuaded to try something based off of someone saying they thought it was good when they tried it, phishing emails will try to appeal to this similarly by targeting areas of interest and say others like you have joined and enjoy it (Siddiqi et al., 2022). They go on to explain how even without new technologies, well defined authorized use policies, operational policies, and informational campaigns have proven to be effective at reducing frequency of social engineering attacks succeeding (Siddiqi et al., 2022). Psychological studies are also great for relating research in other fields like criminology, explaining possible motivations for hackers such as thrill, emotion, or profit (Umphlet, Module 12), and

Criminology and cybersecurity are growing in need of collaboration as more crime moves online, the ability to commit cyber-crimes outside boundaries of jurisdictions and stay anonymous has empowered individual criminals to take on larger organizations as well as countries conduct warfare more covertly for less money. One area that needs collaboration between criminology and cybersecurity is white collar crime, or crimes committed within the workplace (Umphlet, Module 13). There are important insights given by criminological reports on white-collar cybercrime such as the nature of victimization, especially victimology (Umphlet, Module 13). One notable observation found by criminologists is that, unlike traditional crime, victims of white-collar cybercrime often do not know they have been victimized (Dupont & Whelan, 2021). This is important to information security analysts as it shows that when an incident has occurred, extensive checks of previous logs are important to know when the incident started, it can also give insight into what current operations have weaknesses that failed to detect any abnormalities. The amount of crime committed without officials' knowledge is referred to by criminologists as the “dark figure”, and that this variable is “much larger for white-collar crime than it is for other forms of crime” (Hamerton, 2020). Criminology reports have also given insight into demographic of cyber-crime offenders, type of crime committed, and legal action taken against them (Hamerton, 2020). These insights can help with management of incidents for information secuurity analysts as it is possible for them to see what the most likely demographic is to narrow down potential suspects, and if pursuing legal action is worth the investment when weighted against the extra time and labor costs for gathering evidence.

The value of social science economics is especially useful to information security analysts during planning stages. It can be difficult to communicate the need for costly system upgrades, training, and adherence policy structures when the profit motive is the main concern of stakeholders. “Establishing stakeholder partnership and collaboration of key players” is essential for any program for adherence and properly securing resources, and the best way to do that is to tie the profit motive to security (Umphlet, Module 9). Conducting a proper costs/benefits analysis can show possible routes that maximize outcomes without requiring too many recourses (Umphlet, Module 11). Doing this helps establish a culture of security within the workplace from a top-down approach, with stakeholders approving budgets for expanding security operations, to leaders within the organization creating policies and adherence strategies, to individual employees and groups utilization of tools given for secure operations (Umphlet, Module 9). One way this can be communicated is through bug-market organizations that show the minimum cost of known vulnerabilities and open markets for reports of new vulnerabilities (Anderson & Moore, 2006) such as current ransomwares that are affecting competing companies and their losses incurred from halting operations, any litigation that occurred because of the loss of private information, and any possible payouts to be able to resume activities (Umphlet, Module 13). It is also good to show cost effectiveness of certain programs and possible motivating factors, such as a study on bug bounties that found that those that report vulnerabilities for a reward found that the rate and severity of reports did not change with different levels of rewards for most industries, showing that there may be external motivating factors aside from financial as to why these grey-hat hackers operate in such a manor; that same study did also find that certain industries such as ones in the financial and real estate sectors received significantly lower bug reports which also shows that there may be a point of potential financial gain that sways these same actors (Sridhar & Ng, 2023).

The last major social science field I will be discussing is the relationship between cyber security and law. It is important for anyone within cyber security to be aware of current laws, policies, and regulations as it draws the baseline of expectations required before being considered negligence as well as define jurisdictions of control and international cooperation. Baseline expectations are especially important to note as underperformance can be considered deviant behavior and can bring attention to failures within the practice (Umphlet, Module 12). This falls in line with deterrence theory as applied to organizations, establishing guidelines and expected outcomes under normal circumstances prevents organizations from putting others at risk due to the legal risk they incur from not meeting expectations (Umphlet, Module 12). They also incur risk of private lawsuits form consumers that were affected by their negligence, while many of these often do not pan out in the consumers favor, when a breach is large enough it can gain traction and as more people join it can be a big loss both for legal fees and payouts after settlements (Hanson, 2008). There is also a level of trust that consumers put into these businesses, especially when the business has a privacy policy that states practice of protecting consumer information, breaches can be a direct violation of their own privacy statement and may hold the company liable on a larger stage such as a federal investigation (Hanson, 2008).

From the standpoint of an information security analyst, it is an integral part of the career to pull from these different areas of expertise, they can give valuable insight into the current state of the world and how their actions and the actions around them can affect the safety of consumers against cyber criminals. Understanding how to utilize this information to effectively communicate the need for certain processes, how it benefits the organization and the consumers alike, how to understand their own shortcomings and consequences of them. As an information security analyst, it is not just your job to protect information within the organization, it is also your job to make sure standards are being upheld in accordance with the law, and you are contributing to security practice by reporting information found to proper authorities and working with authorities in the event of major cyber events for the safety of the consumer and the organization.

**References**

Anderson, R., & Moore, T. (2006). The Economics of Information Security. *Science*, *314*(5799), 610–613. <https://doi.org/10.1126/science.1130992>

Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Journal of Criminology*, *54*(1), 000486582110039. <https://doi.org/10.1177/00048658211003925>

Hamerton, C. (2020). White-Collar Cybercrime: Evaluating the Redefinition of a Criminological Artifact. *JOURNAL of LAW and CRIMINAL JUSTICE*, *8*(2). <https://doi.org/10.15640/jlcj.v8n2a6>

Hanson, J. (2008). Liability for Consumer Information Security Breaches: Deconstructing FTC Complaints and Settlements. *Washington Journal of Law, Technology & Arts*, *4*(4), 11. <https://digitalcommons.law.uw.edu/wjlta/vol4/iss4/4/>

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences*, *12*(12), 6042. <https://doi.org/10.3390/app12126042>

Sridhar, K., & Ng, M. (2023). *Hacking for good: Leveraging HackerOne data to develop an economic model of Bug Bounties*. Oup.com. <https://academic.oup.com/cybersecurity/article/7/1/tyab007/6168453>

Umphlet, M. (n.d.-a). *CYSE201S Module 9*. Retrieved July 31, 2024, from https://docs.google.com/presentation/d/1eNx0mEG5XH4AxnSm4tR\_q9H0kvrDbWkLXLzSgIZkAtg/edit#slide=id.p21

Umphlet, M. (n.d.-a). *CYSE201S Module 10*. Retrieved July 31, 2024, from <https://docs.google.com/presentation/d/1d1Au262TDvUJi7hxmvawUXkiQQoi9UbGj6wMP2-KNLc/edit#slide=id.p3>

Umphlet, M. (n.d.-a). *CYSE201S Module 11*. Retrieved July 31, 2024, from https://docs.google.com/presentation/d/1dE57qjUiae\_TVXZJiEqpNuAv1\_YCmHo4hUqxj\_bSK24/edit#slide=id.p9

Umphlet, M. (n.d.-a). *CYSE201S Module 12*. Retrieved July 31, 2024, from https://docs.google.com/presentation/d/1hEa51JB3tut23mpO0HT\_KRDB-f\_LzUR4HUTfFoRXgd8/edit#slide=id.p22

Umphlet, M. (n.d.-a). *CYSE201S Module 13*. Retrieved July 31, 2024, from https://docs.google.com/presentation/d/1s7EJVbKyWeUPbaiFndzJP3SUvXJcr8edkD1HyDnsvOw/edit#slide=id.p23