Journal Entry’s 11-15

JE 11

She talks about how cybersecurity analyst are scenically the first line of defense They usually monitor the network or the respond to incidents. As a cybersecurity analyst you are mainly going to be working on preventing phishing attacks, intrusions, monitoring networks. You may also assist in the remediation of venerability's and also providing training for user awareness. There are many different types of analyst so the type of work will vary depending on the focused field.

JE 12

Prospect Theory- Customers reading this letter may overestimate the threat or impact of the breach because it involves a potential loss (identity theft or financial harm). Even if no fraud occurred, the possibility creates anxiety, which could damage trust in the company.

Cognitive Dissonance Theory- Customers trusted this business to keep their information safe. Learning that their trust has been broken. That discomfort might lead customers to avoid future purchases or seek reassurance (calling the company or canceling their card).

Information Asymmetry- The company (and its platform provider) knew about the breach before customers did but customers were only informed after law enforcement allowed it. This delay creates a gap in information, reducing consumer trust and potentially harming the business’s reputation.

Transaction Cost Economics- The breach raises payment costs for customers. Now they may need to monitor bank accounts, replace cards, and deal with potential fraud. This makes buying from the company more expensive in effort and risk, possibly preventing future purchases.

JE 13 This paper shows new research using HackerOne data from 2014–2020 (3,800+ observations) to analyze which companies benefit most from bug bounties. Using 2SLS regression and other econometric tools, the authors find:

Hackers are price insensitive- low bounty budgets can still yield results.

Company size and reputation don’t significantly affect the number of reports.

Finance, retail, and healthcare companies get fewer reports.

New programs don’t reduce reports to older ones.

Programs receive fewer reports over time, unless they expand their scope.

Despite these insights, 40% of report variation remains unexplained, suggesting that much more research is needed to understand bug bounty dynamics.

JE 14

The top 5 most illegal acts out of this list is, Sharing Passwords, Addresses, or Photos of Others, Bullying and Trolling, Faking your identity online, collecting information about children online, and illegal searches on the internet. I chose these options because all of them can lead to facing some sort of possible jail time. I also picked these ones because other than the initial offence it's self, a person can commit more than one act trying to commit a specific act.

JE 15

The career of digital forensics investigators relates with social sciences in a couple of ways, especially since it relates to understanding human behavior, ethics, law, and societal impact. First they need to Understand the motives of the person. Investigators need to know why individuals commit cybercrimes, which relates to criminology and psychology. They also need to Understand social systems, Investigators need to understand how social networks and organizational structures impact security practices and breaches. Lastly the need to understand Legal frameworks, digital forensics operates under legal boundaries. They need to know how evidence must be collected, preserved, and presented. They would need to have a deep knowledge of criminal and civil law.