DB #10

As technology continues to advance and becomes more integrated into our daily lives, it's not surprising that cybercrime is occurring more frequently than ever before. However, despite the rise in cybercrime, it remains difficult to accurately estimate how many incidents occur in the United States each year. There are several potential reasons for this. One possible reason is that people often aren't aware that they are falling victim to a cyberattack. Additionally, those who do realize they've been targeted may feel embarrassed, especially if they fell for scams or other deceptive tactics. In other cases, victims may choose not to report the crime due to potential complications such as reputation damage. For example, businesses that experience cyberattacks might avoid disclosing the incident out of concern that it will erode public trust and harm their brand. While the company may have suffered damages, the loss of customer confidence and future business could prove even more costly.

Lastly, people may also be reluctant to report small-scale cybercrimes due to the lack of effective post-incident management strategies and available resources. Although these types of incidents occur frequently, many law enforcement agencies—especially at the local level—are not adequately equipped to investigate them or bring the perpetrators to justice.

"Cyber-Crime Cases: Why Are Hacks Going Unreported?" *Matthijssen Business Systems*, www.mattnj.com/news-events/cyber-crime-cases-why-are-hacks-going-unreported

Links to an external site.

.

DB #9

Economics play a vital role in the cybersecurity field. One example would be how criminals are often motivated by some type of financial gain. Criminals will weight the potential payoff of an attack versus the likelihood of being caught or penalized. This dynamic creates a "cybersecurity market" where both attackers and defenders adapt to each other's strategies (Moore, 2010).

Another way that economics and cybersecurity can be related it is the form of terrorism. Criminals can target a specific groups economic system to promote wide spread panic and as well as impact supply and demand needs.

Another important way that economics and cybersecurity are interconnected is through cyberterrorism. Cybercriminals can launch targeted attacks on critical economic infrastructure such as banking systems, stock exchanges, and supply chain networks with the intent to cause widespread disruption. These attacks are often designed not only to steal information or cause immediate damage but to undermine trust in financial institutions and destabilize economic systems.

BD#8

Cybersecurity threats not only affect technology but also influence social behavior, trust, and decision-making. As cyberattacks become more sophisticated, researchers must examine the human side of security. Two questions that I feel would be valuable in addressing and would be:

1. How do data breaches impact consumer trust in organizations, and what factors influence trust recovery after a cyberattack?
   When companies suffer security breaches, customers often lose confidence in their ability to protect personal

information. Researching how organizations can rebuild trust through transparency, compensation, or stronger security policies can help businesses retain consumer confidence after an attack.

2. How do cultural differences influence individuals' attitudes toward cybersecurity and risk perception?
   Cybersecurity awareness and behavior vary across cultures due to differences in education, government policies, and digital habits. Understanding how cultural perspectives shape cybersecurity practices can help develop globally effective security awareness programs and policies.

By exploring these questions, organizations can gain insight into the societal impact of cybersecurity and develop strategies to improve trust, awareness, and resilience in the digital world. In addition to the proactive benefits, I believe that it would also provide the general public with some assurance that there were policy and procedures in place to ensure their safety in the event of a security incident.

BD#7

After watching this video, one of my biggest takeaways is how he managed to achieve fluency independently and at such a young age. While it was mentioned that both of his parents work in the tech industry likely giving him some exposure to this skillset, I highly doubt they taught him how to hack into systems. He is undoubtedly highly intelligent and clearly passionate about the field. However, it's concerning to consider how easily someone with malicious intent could acquire this level of expertise.

It was also incredible to see how quickly he was able to access the reporter's information through a Wi-Fi network. This connects to some of the key points discussed in the TedX video we watched, particularly the concept of the human firewall. When he says, "I will never sign into a public Wi-Fi server that I don't

know," it serves as a great example of the human firewall principle we learned about.

DB#6

Rob May emphasizes how individuals play a significant part in protecting themselves against cyber threats. He discusses how though organizations do have systems in places to protect against cyber threats, the biggest weak point in the "firewall" is the users ability to reduce risky behavior. He points out that while organizations heavily invest in technical security solutions like hardware firewalls and software protections, the most significant vulnerability rests with people. During the presentation, he also shows how easily personal information can be obtained disclosed and how this can lead to varying types of attacks. One of his major points that I agree with the most is the need for organizations to invest more time and effort into their organizations members being that they are not only the first line of defense but also the weakest link in preventative practices.

DB#5

I think that the theory that best explains cybercrime is the neutralization theory. The reason being is that it provides insight into the cognitive processes behind cybercrime. Rather than simply labeling offenders as "bad apples," it acknowledges that many individuals who commit cybercrime may perceive their actions as morally acceptable

DB#4

Victim precipitation refers to how a victim's actions or behavior might contribute to an offender's initial attack. While this is not always the case, certain behaviors can increase a person's vulnerability to victimization. For example, practices such as sharing passwords, reusing passwords, using unsecured networks, engaging in risky browsing behavior, and lacking recovery measures can heighten the risk of becoming a victim. Victimization can occur in various forms, including personal, professional, and financial.

DB#3

While security breaches caused by human error can never fully be eliminated due to flawed human nature as well as evolving technology, there will always be areas in which common practices can be improved. Arguably the most important step in incident management is continuous education on awareness along with standard operating procedures. Ensuring that all levels and positions held within an organization have appropriate training based on their position is key in early recognition. Regardless of the scale of an incident where security has been breached, the progression and outcome are largely impacted by the beginning phases. Using an incident of a cardiac arrest as an example, if someone collapses in a public setting, the most important factor in survivability is early recognition, initiation of the appropriate recourses (Emergency Medical Services) and effective CPR. Those three steps usually are not done by medical professionals. However, they play the largest role in patient outcome. In relation to security breaches, there should be a similar approach. The recognition of a security breach can, and often times will be from a non-security specialist. Training non-security specialist to be confident in their skills of recognition will improve the time between the recognition of a possible security breach and the appropriate resources (IT) being "dispatched" to mitigate the incident. Early recognition along

with a strong understanding of standard operating procedures is key in the mitigation of security breach incidents.

In regards to reducing human error resulting in security breaches, it is important to provide awareness training to new and existing employees. In my opinion, most security breaches resulting from human error are rarely a result of gross negligence or malice. I believe that though there are incident of gross negligence or malice, most errors are just complacency, lack of education or lack of experience. If more emphasis can be placed on the importance of simple safe practices such as the use of secure networks, password sharing, the proper securing of data/ personal information and safe application use, the amount of security breaches can be reduced significantly.

DB#2

Determinism as it relates to computer hacking essentially is the idea that an action is caused based on previous reactions or results. Why someone chooses to engage in "hacking" varies for many different reasons. However, there is typically some type of benefit or gain to be had in participating in the act. With that being said, most of the time the person committing the act has either personally experienced, or witnessed some form of gain to be had. Additionally, a systematic approach is either developed or witnessed to ensure consistency, predictability and success or the act. The predictably of both the process as well as the outcome greatly influence ones drive to engage in activities such as hacking.