CIS-481: Introduction to Information Security
Module 6 - Legal, Ethical, and Professional Issues
Exercise #5 - Option C

Team: 3
Participants: Ashley Aguilera Rico, Raveen Bryant, Ryan Foster, Yen Hsieh Hsu, Abby Nguyen

Logistics

A. Get together with other students on your assigned **Team** in person and/or virtually.
B. Review the three options available and decide on only one to pursue as a team.
C. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning and may impact your performance on assessments, especially with respect to the essay questions.
D. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

Problem 1
The FBI maintains an extensive site dedicated to cybercrime:

https://www.fbi.gov/investigate/cyber

Related is the FBI's Internet Crime Complaint Center:

https://www.ic3.gov/

1. What is the FBI's stated cyber strategy and primary goal of this strategy (linked here)? (*5 points)*

   The FBI's main cyber strategy is to impose risk and consequence on illegal and fraudulent cyber behavior that intentionally infringes upon the security architecture. The goal of this strategy is to set a precedent that criminal attempts to harm and compromise federal, financial, and public information security systems are unacceptable and handled with high priority. This will hopefully in result deter criminals and encourage safer web experiences.

2. From the 2021 Internet Crime Annual Report, review the last five years of complaints (2017 – 2021) on p. 7 of the report.
    a. What is the percentage change in complaints from 2017 to 2021? Is this what you expected? Why or why not? (*5 points*)

        From 2017 to 2021, the number of complaints have increased by 180.98%. The massive increase in complaints was to be expected as the growth in technology use in individuals and businesses results in the risk of cyber attacks and malicious cyber activity becoming more prevalent. Even though individuals and businesses have ways to protect themselves and may be aware of such crimes, it does not prevent criminals from using various methods, where some may look legitimate and trustworthy to individuals and business owners, to commit the crime.

3. From the 2021 Internet Crime Annual Report, the FBI notes that in 2021 the IC3 received 19,954 Business Email Compromise (BEC)/ Email Account Compromise (EAC) complaints with adjusted losses of nearly $2.4 billion.
    a. What is the difference between Business Email Compromise (BEC) and Email Account Compromise (EAC)? Appendix A on p. 30 has definitions. (*5 points*)

        Essentially, Business Account Compromise (BEC) entails the targeting of businesses working with foreign suppliers that do regular wire transfer payments. Email Account Compromise (EAC) is a similar scam that entails much of the same but instead focuses on individuals rather than businesses. Both types of scams are carried out by fraudulent means that compromise email accounts through social engineering attempts or using computer intrusion methods to conduct unauthorized transfers of funds.

    b. How has COVID-19 affected the techniques that fraudsters are using to execute BEC/EAC schemes? See the threat overviews beginning on p. 9 of the report. (*5 points*)

        COVID-19 led to a massive uptick in telework and virtual meetings. The techniques have evolved in the sense that fraudsters have started to compromise an employer or financial director's email which would then be reused to participate in virtual meetings with said employees. The fraudster could then insert stills of the CEO with and impersonate the CEO and claim that their audio was not working. The virtual meeting could then be used to instruct employees to initiate wire transfers or provide wiring

instructions. Overall, COVID-19 and the massive increase in virtual meetings has provided fraudsters with many more opportunities to impersonate business managers or employees with more success. In-person meetings prevented much of this for obvious reasons.

4. From the 2021 Internet Crime Annual Report, the FBI notes that in 2021 the IC3 received 34,202 complaints involving the use of some type of cryptocurrency, such as Bitcoin, Ethereum, etc. The loss amount reported in IC3 complaints increased nearly seven-fold, from 2020's reported amount to total reported losses in 2021 of more than $1.6 billion.
    a. How do cryptocurrency support impersonators commonly execute their fraud? See the Cryptocurrency threat overview on p. 13 of the report. (*5 points*)

       They'll send an alert to the owners of cryptocurrency wallets making them aware of an "issue," which leads them to getting convinced to give access to their crypto wallet, or transfer its contents to another wallet, in order to "protect" their contents. The owners look for customer support numbers to help them with their accounts, but accidentally call a fake crypto customer service number that gets them to give up their login info and/or control of their accounts.