**CIS-481: Introduction to Information Security**

**Module 6 - Legal, Ethical, and Professional Issues**

**Exercise #5 - Option C**

**Team: 3**

**Participants: Dustin Thompson, Bryce Watson, George Flarsheim, Bradley Lawton, Destinee Matsoumou**

**Logistics**

1. Get together with other students on your assigned **Team** in person and/or virtually.
2. Review the three options available and decide on only one to pursue as a team.
3. 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.
4. 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](https://www.fbi.gov/investigate/cyber))? (*5 points)*

The FBI’s cyber strategy is to impose risk and consequences on cyber adversaries. The goal of the FBI is to change the behavior of criminals and nation-states who believe they can compromise U.S. networks, steal financial and intellectual property, and put critical infrastructure at risk without facing risk themselves.

1. From the [2021 Internet Crime Annual Report](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf), review the last five years of complaints (2017 – 2021) on p. 7 of the report.
   1. What is the percentage change in complaints from 2017 to 2021? Is this what you expected? Why or why not? (*5 points*)

2017: 301,580 complaints

2018: 351,937

2019: 467,361

2020: 791,790

2021: 847,376

Total: 2,760,044

(847,376-301,580)/301,580=180% increase.

This increase is to be expected with the rapid change to work from home and an increase in digital business caused by the pandemic. With the sudden change to digital work many new people who were not digitally literate were pushed into positions which they did not have the proper security training. This is shown with the increase in phishing style scams shown on page 9.

1. From the [2021 Internet Crime Annual Report](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf), 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.
   1. What is the difference between Business Email Compromise (BEC) and Email Account Compromise (EAC)? Appendix A on p. 30 has definitions. (*5 points*)

Business Email Compromise (BEC) is a scam that targets businesses and not individuals. It employs the use of wire transfer payments or gift cards with an email eiminating from an outside source. Email Account Compromise (EAC) is similar to the BEC scam, but utilizes compromised emails to send the scam, e.g. an individual or someone’s company email is hacked and used.

* 1. 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*)

During the COVID-19 pandemic more people and companies used online, or virtual, meetings. These online meetings are now being compromised with BEC/EAC schemes. Infiltrators are gaining access to CEOs or CIOs and pretending to have online meetings. In these meetings the infiltrators ask for wire transfers or gift cards.

1. From the [2021 Internet Crime Annual Report](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf), 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.
   1. How do cryptocurrency support impersonators commonly execute their fraud? See the Cryptocurrency threat overview on p. 13 of the report. (*5 points*)

Cryptocurrency support impersonators commonly use phishing to execute their fraud. They pretend to be tech or support personnel from the crypto company and convince them that their crypto is at risk and needs to be secured by transferring it into a different wallet. They also create fake websites. Victims access these fake websites thinking the information they are providing is safeguarded, that their crypto is safe, but in reality, they are being robbed.