CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #3 - Option D

Team: 5
Participants: Ethan Grimes, Holli Grubbs, Gregory Ellis, James Hoagland

Logistics

A. Get together with other students on your assigned team in person and virtually.
B. Review the four 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.
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 are the FBI's key priorities in preventing cybercrime and abuse? *(10 points)*

   The FBI's main priorities concerning the prevention of cybercrime and abuse include imposing risks and consequences on its adversaries. Other key priorities include computer and network intrusions, identity theft, and fraud. They want to ensure that the risks criminals take to compromise U.S. networks will in turn force them to face severe penalties and risks for doing so. The FBI uses different authorities, methods, and partnerships to punish cyber adversaries. Laws the FBI use to persecute cybercrime and abuse include the USA FREEDOM Act, an amended act based off powers granted through the USA PATRIOT Act. The severity of the punishments depend on the value of what information was obtained and whether the crime was committed for purpose of commercial advantage, private financial gain, and furtherance of a criminal act. Victims of cybercrime should file a report with the Internet Crime Complaint Center. The reports are used for investigations and for intelligence.
   The FBI is also required to protect its own information assets through the FISMA act. The Federal Information Security Management Act mandates that all federal agencies establish information security programs that include policies and procedures for their employees to follow.

2. Review the most recent Annual Report of FBI's Internet Crime Complaint Center. Describe the 5 previous years' complaint statistics. *(5 points)*

2019:

-Total of 467,361 complaints with losses estimated around $3.5 billion.
-The most frequent crimes were Phishing, Non-Payment/Non-Delivery, Extortion, and Personal Data Breach.
-The crimes that were reported with the highest losses were BEC (Business Email Compromise), Confidence/Romance Fraud, and Spoofing
-In IC3's Recovery Asset Team (RAT) first full year of operation they were able to recover over $300 million lost to online scams which was a 79% return rate of reported losses.

2018:

-Total of 351,937 complaints with losses estimated around $2.7 billion.
-The most frequent crimes were Non-Payment/Non-Delivery, Extortion, and Personal Data Breach.
-The crimes that were reported with the highest losses were BEC, Confidence/Romance fraud, and Non-Payment/Non-Delivery.
- There were 1,061 DFFKC's (Domestic Financial Fraud Kill Chain) totaling $257,096,992 which was a recover rate of 75%.
- OWS (Operation Wellspring) task force opened 18 investigations in 2018

2017:

-Total of 301,580 complaints with losses estimated around $1.4 billion.
-The most frequent crimes were Non-Payment/Non-Delivery, Personal Data Breach, and Phishing.
-The crimes that were reported with the highest losses were BEC, Confidence/Romance fraud, and Non-Payment/Non-Delivery.
-The 4 millionth consumer internet crime complaint was reported this year.
-OWS task force opened 27 investigations in 2017.

2016:

-Total of 298,728 complaints with losses estimated around $1.3 billion.
-The most frequent crimes were Non-Payment/Non-Delivery, Personal Data Breach, and Payment Scams.
-The crimes that were reported with the highest losses were BEC, Romance and Confidence Fraud, and Non-Payment/Non-Delivery Scams.
-OWS task force opened 37 investigations in 2016.

2015:

-Total of over 8,000 complaints with losses estimated around $275 million
-IC3 provided 165 referrals to Cyber Task Forces (CTFs), which resulted in 39 OWS cases.
-Tracking of EAC Scams began in 2015

3. Based on these, evaluate the effectiveness of applications of cybersecurity in preventing crime and abuse. *(10 points)*

The overall effectiveness of these various applications of cybersecurity in dealing with crime and abuse has not been perfect, according to the statistics of the Annual Report of FBI's Internet Crime Complaint Center. The past five years have shown a steady increase in the statistics of complaints and estimated losses. To contrast, in 2015 there were a total of 8,000 complaints with estimated losses of around $275 million, whereas in 2019 there were a total of 467,361 complaints with estimated losses of 3.5 billion.

Although there has been a noticeable rise in complaints and losses regrading cyber-attacks, these numbers would certainly be much higher if not for the FBI's main priorities with the prevention of cybercrime by imposing risks and consequences on its adversaries with their various methods and authorities. The FISMA act requires agencies to evaluate the effectiveness of their information security program no less than every year, but as we learned in chapter four that companies fail to prioritize reviewing policies and procedures regarding information security and implement changes based on new security risks.