Reading assignment: Read Chapter 1: Connected, Dependent and Vulnerable from the Future Crimes book. Prepare responses to the following questions.

1. Investigate the password reset process for each of the following services: Gmail, Facebook and iCloud. Document your findings in the form of a visual or flowchart. (Three students will be chosen randomly to present their findings on the board).

Gmail

1. Head to the Gmail sign-in page and click the “Forgot Password” link.
2. Enter the last password you remember. If you can't remember one, click “Try a different question.”
3. Enter the secondary email address you used when you set up your Gmail account to get a password reset email.

Vulnerability: This process is vulnerable if someone knows the recovery email/secondary email address that the account holder uses. If so, it would be easier to rest the user’s password and even change the recovery/secondary email address inhibiting the user from accessing his/her account.

Facebook

1. Open facebook.com
2. Click forgot account located under the login field and enter your email
3. Facebook sends you a code to enter
4. Put your new password/skip this step to log in

Vulnerability: If someone know the account owner’s email address, they can easily get access to the user’s account and even change their password.

iCloud

1. Navigate to iforgot.apple.com in any web browser.
2. Enter your Apple ID email address and click Continue.
3. Select I need to reset my password and click Continue.
4. Select Get an email or Answer security questions.
5. Click Continue.
6. Click Done

Vulnerability: The option to use an email to rest the password allows someone who has a user’s email address to easily reset the password. This process is especially easier if the account holder uses the same email for both the apple ID and the rest process.

2. For question 1 above, outline vulnerabilities in the password reset process for each of three platforms.

\* See question 1 above.

3. What is the Westphalian treaty? How effective was it in a world where borders regulated commerce and information exchange?

The Westphalian treaty was a system that allowed countries to be sovereign in their territory, with no role for outside authorities to meddle in a nation’s domestic affairs. It was fairly effective to establish controls in a world where borders regulated commerce and information exchange.

4. Why is the framework of the Westphalian treaty not as effective anymore?

The framework of the Westphalian treaty is not as effective anymore due to the fact that physical borders are less clear in the online world. This scenario, in turn, has also allowed criminals to freely enter and exist any virtual location as they please.

5. On page 15, the author compares two incidents: an attempted bank robbery at a bank location in New York's Time Square, and the 1994 Internet bank robbery. Compare and contrast the two. What role does digital forensics play with the latter?

Attempting a bank robbery at a bank location (such as in New York's Time Square) would require penetrating a physical location, breaching state and national laws. Attempts to solve the case would require gathering physical evidence that was left behind at the scene of the crime by the robber including fingerprints, DNA, and images taken by the security cameras. On the other hand, in the 1994 Internet bank robbery, it is hard to gather evidence as no fingerprints or DNA was marked. Additionally, the robber never needed physical access to execute the crime. Digital forensics plays a critical tole with the Internet robbery by allowing forensic experts to collect, analyze, recover, and investigate material found in digital devices to solve the crime and resolve an issue.

6. What were the motivations of the Alvi brothers in creating the Brain virus?

The motivations of the Alvi brothers in creating the Brain virus was to stop others from pirating the software the brothers had spent years developing.

7. Research the Brain virus. Prepare a response about origin, extent of damage, counter strategies that were executed to limit or terminate its impact.

The Alvi brothers were operating a computer store in the Pakistani city of Lahore when they noticed pirated copies of a computer program they had written being circulated by their customers. To teach their customers a lesson, they created the Brain virus. Written in Jan 1986, the virus was created solely for addressing illegal copies of their program and it was  intended to ensure that users whose machines had become infected due to using pirated software could contact them for vaccination (Harán, 2018).

The extent of the damage included It alterting the boot sectors of floppy disks, possibly corrupting files in the process. It also spread to any uninfected floppy disks inserted into the system. Since that time, numerous variations of this virus have been reported. The virus was hard to detect, not easily destroyed or deactivated, spread infection widely, re-infected its home program or other programs, easy to create, and machine independent and OS independent (Harán, 2018).

Brain Virus infected a lot of machines around the globe. IBM took very serious action against the brothers and, eventually, they stopped distributing the virus with the medical software. Nowadays, they’re running a company named Brain Telecommunication Limited providing Internet services at the same address (Harán, 2018).

8. Find out the latest Gartner estimate for spending on software security.

Gartner forecasted the worldwide information security spending to Exceed $124 Billion in 2019 previously. Now, the organization asserts that the global IT spending is expected to reach $3.9 Trillion in 2020. This spending is an increase of 3.4% when compared to the 2019 forecast (Gartner, 2019).

9. Research any three zero-day vulnerabilities. Your research should focus on origin, extent of damage, counter strategies.

A list of the latest zero-day vulnerabilities with their details can be found here: <https://www.zerodayinitiative.com/advisories/published/>

10. Research the 2019 Verizon Data Breach Investigations Report. Be prepared to talk about key findings.

The key findings of the 2019 Verizon Data Breach Investigations Report can be found here: <https://www.hipaajournal.com/2019-verizon-data-breach-investigations-report-findings/>

The 2019 Verizon Data Breach Investigations Report can be found here: <https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf>

11. Why are companies loathe to admitting a breach? The book discusses this at length. Be prepared to talk about 5-6 reasons why admitting a breach poses different kinds of liability issues for companies.

Companies loathe to admitting a breach and deny it as slog as possible because the fees for consequences such as replacing credit card, purchasing consumer credit-monitoring services, and rising cyber-insurance premiums can escalate.

Admitting a breach poses different kinds of liability issues for companies because there are even greater costs in addition to the ones above such as

1. Stock market price drops
2. Class-action lawsuits from customers, regulators, and shareholders
3. Costs for every record stolen (which grows the cost exponentially when a lot of account records are stolen)
4. Costs due to technological insecurity (Ineffective security)
5. Costs from growing connectedness on penetrable technologies

12. Research the 2007 TJX hack. Discuss key findings.

The TJK hack has been revealed as the biggest ever breach of personal data. U.S. Securities Exchange Commission filings by the firm show that 45.7m credit and debit card numbers were stolen over a period of 18 months. Albert Gonzalez was sentenced to 20 years in prison for leading a gang of cyberthieves who stole more than 90 million credit and debit card numbers from TJX and other retailers.

References

Harán, J. (2018). Malware of the 1980s: Looking back at the Brain Virus and the Morris Worm. Retrieved from https://www.welivesecurity.com/2018/11/05/malware-1980s-brain-virus-morris-worm/

Gartner. (2019). Gartner Says IT Spending in EMEA to Return to Growth in 2020. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2019-11-07-gartner-says-it-spending-in-emea-to-return-to-growth-in-2020