**MIS 310 Week 10 Homework (30 points)** Name: Megan Leonard

You will not be given credit for answers that are copies or near verbatim transcripts – please use your own words and document sources where appropriate using proper APA guidelines. Apply the principles learned in this chapter (chapter 9) or previous chapters to answer the questions for this assignment.

**Chapter 9 Learning Outcomes**

|  |
| --- |
| * Explain why computer incidents are so prevalent. * Identify and briefly describe the types of computer exploits and their impact. * Describe the earmarks of a strong security program. * Identify specific measures used to prevent computer crime. * Outline actions that must be taken in the event of a successful security intrusion. |

**Week 10 Review Questions (10 points)**

Answer the following questions in one or more paragraphs using proper APA format as required**:**

1. [2 points] What is BYOD? What security issues does it raise?

BYOD means bring your own device, this means that the person is in charge of acquiring a device to use for the task at hand. The security issues with this are that the devices can be taken home to a not as safe location and each device would not have the same level of safety. For instance, if one person does not have antivirus software and gets a trojan file mixed into their work, then it could be unknowingly sent or spread through the network while that device acts as a door into the company or group information.

1. [2 points] What is the difference between a black hat hacker and a cracker?

The difference between a black hat hacker and a cracker is that the hacker will break security for malicious or illegal gain while the cracker will just cause problems and steal data.

1. [2 points] Outline the steps necessary to conduct an effective computer security risk assessment.

The necessary steps of computer security risk assessment are; identify the important assets, identify the events and risks that could cause the loss of assets, assess the likelihood of each potential threat happening, determine the impact the threat would cause, determine how each threat can be lessened, see if these ideas can be used, check the cost-benefit analysis, and finally make the decision on the implementation.

1. [2 points] What is meant by a layered security solution? Identify several layers of protective measures commonly employed in many organizations.

Layered security solution is a means of security that has several different stages that a hacker would need to get through for instance to access a computer the hacker may need to break through the network firewall then have the next layer of the computer firewall. Possible layers of protection include firewalls, security dashboards and antivirus software.

1. [2 points] What is a managed security service provider (MSSP)? What sort of services does such an organization provide?

MSSP is a security company that works on monitoring and maintaining the security of networks and computers for other companies. The services that it provides include; vpns, antivirus, firewall, and intrusion detection.

**Week 10 Critical Thinking Exercise (10 points)**

Read the following and answer the questions in one or more paragraphs using proper APA format as required**:**

***Spear-Phishing Attack!***

*It appears that someone is using your firm’s corporate directory—which includes job titles and email addresses—to contact senior managers and directors via email. The email requests that the recipient click on a URL, which leads to a Web site that looks as if it were designed by your Human Resources organization. Once at this phony Web site, the employees are asked to confirm the bank and account number to be used for electronic deposit of their annual bonus check.*

1. [2 points] How is this attack different from an ordinary phishing attack?

The difference between phishing and spear-phishing is that spear-phishing is targeted to a group of workers in an organization.

1. [2 points] Craft a communication that might be sent out to employees to thwart this attack.

All emails sent with only a link and not using proper organization email should be reported to the security sector and the imitated section.

1. [3 points] Should this communication come from Human Resources, the corporate information systems security organization, or some other entity?

To start, human resources should send out the message as they are the ones being imitated. Once they have sent the message then the security organization would be able to send a message about how they are dealing with this and what to do for future situations.

1. [3 points] What actions can be taken to lessen the potential impact of future such attacks?

Actions that can be taken to lessen future attacks is add certain safeguards in the emails the section of the companies send and receive. For example, some sites will have a certain way of sending emails whether it is specific wording or images, emails without the official safeguards would be ones that would be reported to the specific section it is imitating so if it is real, it can be fixed and resent and if false it can be reported.

**Week 10 Case Study (10 points)**

Read the following and answer the questions in one or more paragraphs using proper APA format as required**:**

***Sony’s Response to North Korea’s Cyberattack***

*On November 24, 2014, employees of Sony Pictures Entertainment booted up their computers to find an image of a skull along with a message from a group calling itself the Guardians of Peace. The message read: “We’ve already warned you and this is just the beginning. We’ve obtained all your internal data including your secrets and top secrets [which will be released] if you don’t obey us.”*

*As Sony would eventually discover, the hackers had stolen reams of sensitive data, including the Social Security numbers of 47,000 current and former employees, system passwords, salary lists, contracts, and even copies of some Sony employees’ passports. The hackers accessed hundreds of Outlook mailboxes as well as Sony IT audit documents. They also stole media files and placed pirated copies of five of Sony’s movies on illegal file-sharing servers. Sony was forced to completely shut down its information systems in an attempt to stem the data breach. Ultimately, Sony would determine that the damage done by the hackers was far more extensive than it first believed. Not only had data been stolen, but 75 percent of the company’s servers had been destroyed and several internal data centers had been wiped clean.*

*Contacted within hours of the event, the FBI soon identified the culprit. In June, several months before the hack, North Korea’s Ministry of Foreign Affairs had declared that it would take “a decisive and merciless countermeasure” if the U.S. government did not prevent the planned release of Sony’s motion picture The Interview, which features two reporters who venture to North Korea to interview and assassinate the country’s dictator, Kim Jong-un. In the film, the main character, initially won over by the dictator’s apparent kindness, discovers that the tyrant is lying about the country’s prosperity and freedoms. The plot, along with the movie’s unflattering portrayal of the dictator as ruthless and childish, had caught the attention of the North Korean government.*

*The U.S. government disclosed that it had proof that the North Koreans had made good on their threat. The U.S. National Security Agency (NSA) had reportedly penetrated the North Korean cyberwarfare unit four years prior to the attack and had been monitoring its capabilities since then. After Sony alerted the FBI of the attack, the NSA was able to trace the attack back to North Korea, using a digital fingerprint the hackers had left in the malware. Several weeks after the attack, FBI Director James Comey, revealed in a speech that the Sony hackers had been sloppy. “We could see that the IP [Internet protocol] addresses that were being used to post and to send the emails were coming from IPs that were exclusively used by the North Koreans.”*

*The hackers warned Sony not to release The Interview, and then on December 16, the group issued a message threatening large terrorist attacks on theaters that showed the film. The National Organization of Theatre Owners contacted the Department of Homeland Security for information and advice. The FBI and NSA released a bulletin explaining that they had no credible information about a plan to attack theaters, but they could neither confirm nor deny whether the hackers had the ability to launch such an attack. Shortly after the bulletin was released, the four largest U.S. theater chains withdrew their requests to show the movie—Carmike Cinemas first, followed by Regal Entertainment, AMC Entertainment, and Cinemark. Within hours, Sony announced that it had canceled the film’s release. White House officials, Hollywood personalities, and the media were aghast. Comedian Jimmy Kimmel tweeted that the decision by the major theater chains to refuse to screen The Interview was “an un-American act of cowardice that validates terrorist actions and sets a terrifying precedent.”*

*On December 19, President Obama addressed the issue publicly: “Sony is a corporation. It suffered significant damage. There were threats against its employees. I’m sympathetic to the concerns that they faced. Having said all that, yes, I think they made a mistake.” Obama explained, “We cannot have a society in which some dictator in some place can start imposing censorship in the United States.” The president’s remarks highlighted the seriousness of the**incident to the American public, many of whom came to view the incident as an attack on the freedom of expression.*

*In response to Obama’s comments, Sony officials released a statement later the same day: “Let us be clear—the only decision that we have made with respect to release of the film was not to release it on Christmas Day in theaters, after the theater owners declined to show it.... After that decision, we immediately began actively surveying alternatives to enable us to release the movie on a different platform. It is still our hope that anyone who wants to see this movie will get the opportunity to do so.”*

*In fact, on Christmas Day, the planned release day in the theater, The Interview became available through video-on-demand outlets such as Amazon.com, and within less than a month, the movie had brought in over $40 million in revenue. Approximately 6 million viewers had rented or purchased the movie in this way. Several hundred movie theaters that opted to screen the movie generated another $6 million. Over the next two months, Sony also released the movie on Netflix, on DVD and Blu-Ray, and in theaters in other countries.*

*Meanwhile, Sony has worked to recover from the damage done to the company itself by the hack. Sony Pictures’ parent company, which is based in Japan, asked regulators there for an extension to file its third-quarter financial results. It also fired executive Amy Pascal whose leaked emails contained derogatory remarks about Hollywood producers and the U.S. president’s movie preferences. The company also provided one year of free credit protection services to current and former employees.*

*In February 2015, President Obama held the first-ever White House summit on cybersecurity issues in Silicon Valley. The summit was billed as an attempt to deal with the increasing vulnerability of U.S. companies to cyberattacks—including those backed by foreign governments. However, the chief executives of Microsoft, Google, Facebook, and Yahoo all refused to attend the summit. Those companies have long advocated for the government to stop its practice of collecting and using private data to track terrorist and criminal activities and have worked to find better ways to encrypt the data of their customers. However, U.S. security agencies have continually pressured the IT giants to keep the data as unencrypted as possible to facilitate the government’s law enforcement work. Ultimately, both the government and private businesses will need to find a way to work together to meet two contradictory needs—the country’s need to make itself less vulnerable to cyberattacks while at the same time protecting itself from potential real-world violence.*

1. [3 points] Do you think that Sony’s response to the attack was appropriate? Why or why not?

I think that the response of pulling the release of the movie was appropriate as their workers faced that threat of doxing using information that can make identity fraud easier. As a company they needed to spend the time and effort to try to recover what they can as well as protect their workers as the data leak would affect their company and 47000 workers and their livelihoods.

1. [3 points] What might Sony and the U.S. government done differently to discourage future such attacks on other U.S. organizations?

To discourage future attacks the U.S. could alter their security and add a layer that acts as a trap. If a person breaks through the first wall of security, then the ip will be followed back and attacked and reported.

1. [4 points] Are there measures that organizations and the U.S. government can take together to prevent both real-world terrorist violence and cyberattacks?

Measures that can be taken to prevent the violence and attacks would be working with different social sites to determine if people are making real threats or joking. For example, there was a killer who used reddit to post about their victims and intents, having the site let people flag these posts as potentially harmful lets the site look into the account of the person and report the person if deemed a threat.

SOURCES: Barrett, Devlin and Danny Yadron, “Sony, U.S. Agencies Fumbled After Cyberattack,” Wall Street Journal, February 22, 2015, www.wsj.com/articles/sony-u-s-agencies-fumbled-after-cyberattack-1424641424; Mitchell, Andrea, “Sony Hack: N. Korean Intel Gleaned by NSA during Incursion,” NBC News, January 18, 2015, www.nbcnews.com/storyline/sony-hack/sony-hack-n-korean-intel-gleaned-nsa-during-incursion-n288761; Schatz, Amy, “Obama Acknowledges Strains with SiliconValley,” SFGate, February 14, 2015, http://blog.sfgate.com/techchron/2015/02/14/obama-acknowledges-strains-with-silicon-valley/; Dwyer, Devin and Mary Bruce, “Sony Hacking: President Obama Says Company Made ?Mistake’ in Canceling ‘The Interview,’” ABC News, December 19, 2014, http://abcnews.go.com/Politics/obama-sony-made-mistake-canceling-film-release/story?id=27720800; Pallotta, Frank, “Sony’s ‘The Interview’ Coming to Netflix,” CNN Money, January 20, 2015, http://money.cnn.com/2015/01/20/media/the-interview-makes-40-million/; Pepitone, Julianne, “Sony Hack: ‘Critical’ Systems Won’t Be Back Online until February,” NBC News, January 23, 2015, www.nbcnews.com/storyline/sony-hack/sony-hack-critical-systems-wont-be-back-online-until-february-n292126; Cieply, Michael and Brooks Barnes, “Sony Cyberattack, First a Nuisance, Swiftly Grew into a Firestorm,” New York Times, December 30, 2014, www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html; “The Interview: A Guide to the Cyber Attack on Hollywood,” BBC, December 29, 2014, www.bbc.com/news/entertainment-arts-30512032; Whittaker, Zack, “FBI Says North Korea Is ‘Responsible’ for Sony Hack, as White House Mulls Response,” ZDNet, December 19, 2014, www.zdnet.com/article/us-government-officially-blames-north-korea-for-sony-hack/; Osborne, Charlie, “Sony Pictures Corporate Files Stolen and Released in Cyberattack,” ZDNet, November 28, 2014, www.zdnet.com/article/sony-pictures-corporate-files-stolen-and-released-in-cyberattack; Osborne, Charlie, “Sony Hack Exposed Social Security Numbers of Hollywood Celebrities,” ZDNet, December 5, 2015, www.zdnet.com/article/sony-hack-exposed-social-security-numbers-of-hollywood-celebrities/; Sanger, David E. and Nicole Perlroth, “Obama Heads to Tech Security Talks amid Tensions,” New York Times, February 12, 2015, www.nytimes.com/2015/02/13/business/obama-heads-to-security-talks-amid-tensions.html; Whitney, Lance, “Sony Seeks to Delay Filing Earnings in Wake of Cyberattack,” CNET, January 23, 2015, [www.cnet.com/news/sony-asks-to-delay-filing-earnings-due-to-cyberattack](http://www.cnet.com/news/sony-asks-to-delay-filing-earnings-due-to-cyberattack).