|  |  |  |
| --- | --- | --- |
| 10 | **.**  **.**  **.**  **.**  **.**  **.**  **.**  **.**  **.**  **.**  **.**  **.**  **.**  **.**  **.**  **.**  **.**  **.**  **..**  **.**  **.**  **.**  **.** | **Information Systems Security** |

|  |  |
| --- | --- |
| CHAPTER LEARNING OBJECTIVE QUESTIONS |  |

10-1 What Is the Goal of Information Systems Security?

10-2 How Big Is the Computer Security Problem?

10-3 How Should You Respond to Security Threats?

10-4 How Should Organizations Respond to Security Threats?

10-5 How Can Technical Safeguards Protect Against Security Threats?

10-6 How Can Data Safeguards Protect Against Security Threats?

10-7 How Can Human Safeguards Protect Against Security Threats?

10-8 How Should Organizations Respond to Security Incidents?

Learning Catalytics™ is a student response tool that helps you generate class discussion, customize your lecture, and promote peer-to-peer learning based on real-time analytics. Learning Catalytics uses students’ smartphones, tablets, or laptops to engage them in more interactive tasks.

|  |  |
| --- | --- |
| SO WHAT? |  |

## Largest! Data! Breach! Ever!

1. *Most data breaches are found within a few days or weeks. Why did the Yahoo! data breach take so long to be discovered? Would the disclosure of the data breach have been harmful to Yahoo!’s efforts to sell their company?*

It is unclear exactly when the data breach was discovered, but it did take over three years for the breach to be disclosed to the public. There is no doubt that disclosure of the breach would negatively impact the company valuation; therefore, the company had an incentive to hide the breach as they tried to find a buyer.

1. *Have you been a victim of one of the large security breaches over the past several years? If so, what was the impact of your data being compromised? Did you have to take any actions to try to secure your data or your identity? Have you continued being a customer (or using the site) of the company that was compromised? (If you have not been a victim, think about how you would likely respond in this situation.)*

Students’ answers will vary, depending on their experience with data breaches. The question about continuing to do business with the company should trigger some interesting classroom discussion.

1. *The article reports that several years transpired between the time when the breach occurred and the time when the breach was acknowledged and made public. Why is there so much latency between the incident and the response?*

The internal discussions taking place at the time are hard to know as an outsider. Companies that choose to delay announcing a breach publicly are usually trying to get their response plans in order so that they can mitigate the negative impact of the breach announcement.

1. *Compare this breach to the Equifax data breach that also happened recently. (If you are not familiar with the Equifax breach, take a few minutes to conduct a search and read about it). Was the Equifax breach or the Yahoo! breach worse? Be prepared to defend your opinion.*

Students’ opinions on the comparative severity of the two breaches will vary. Students may feel the Equifax breach is worse than Yahoo! because of the nature of the personal financial data compromised. However, in both cases, valuable personal information was stolen.

|  |  |
| --- | --- |
| COLLABORATION EXERCISE 10 |  |

*Using the collaboration IS you built in Chapter 1 (pages 25–26), collaborate with a group of students to answer the following questions. If you haven’t built your collaboration IS yet, reread Collaboration Exercise 1 and Chapter Extension 10. Meet with your team and build a collaboration IS that uses tools like Google Docs, SharePoint, or other collaboration tools. Do not forget the need for procedures and team training.*

1. *Search the Web for the term* computer crime *and any related terms. Identify what you and your teammates think are the five most serious recent examples. Consider no crime that occurred more than 6 months ago. For each crime, summarize the loss that occurred and the circumstances surrounding the loss, and identify safeguards that were not in place or were ineffective in preventing the crime.*

Students will find various examples of computer crimes that will change over time. A good source of current examples is the U.S. Department of Justice’s Computer Crime and Intellectual Property section’s Web site. A page with current press releases is available. Two current examples include:

# “Manhattan U.S. Attorney Announces Charges Against Austin Man For Computer Hacking And Fraud Scheme To Steal Unreleased Music From Music Industry Professionals,” A criminal indictment was filed today against Christian Erazo for conspiring with others to commit wire fraud and computer intrusion, as well as committing aggravated identity theft, by hacking a music producer’s social networking account to impersonate the producer in order to solicit and obtain unreleased music from other artists, which he then directed the artists to send to a fake email account in the producer’s name. In addition, ERAZO hacked the online accounts of two music management companies in order to steal unreleased music of numerous music industry professionals. Nov 25, 2019.

# “Russian Hacker Who Used NeverQuest Malware To Steal Money From Victims’ Bank Accounts Sentenced In Manhattan Federal Court To Four Years In Prison,” STANISLAV VITALIYEVICH LISOV, a/k/a “Black,” a/k/a “Blackf” (“LISOV”), was sentenced to 48 months in prison today for conspiring to deploy and use a type of malicious software known as NeverQuest to infect the computers of unwitting victims, steal their login information for online banking accounts, and use that information to steal money out of the victims’ accounts. NeverQuest has been responsible for millions of dollars’ worth of attempts by hackers to steal money out of victims’ bank accounts. Nov 21, 2019.

LO: 2, Learning Outcome: Describe different methods of managing IS security, AACSB: Analytic Skills)

1. *Search the Web for the term* computer crime statistics *and find two sources other than the Accenture surveys cited in section 10-2.*
   1. *For each source, explain the methodology used and explain strengths and weaknesses of that methodology.*

Students will find various sources of computer crime statistics that will change over time. Two current examples include:

* A list of 20 eye-opening cybercrime statistics was found at https://securityintelligence.com/20-eye-opening-cybercrime-statistics/. This is a compilation of crime statistics pulled from a variety of sources.
* The Internet Crime Complaint Center Web site provides annual reports (<https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf> ) that provide a variety of Internet crime statistics. The iC3 is a partnership between the FBI and the National White Collar Crime Center, which is supported through the Bureau of Justice Assistance. These statistics are based on complaints filed with the iC3 and therefore only reflect actual complaints of cybercrime. (LO: 2, Learning Outcome: Describe different methods of managing IS security, AACSB: Analytical Thinking)
  1. *Compare the data in the two new sources to that in section 10-2 and describe differences.*

Student responses will vary depending on the sources found by each team. (LO: 2, Learning Outcome: Describe different methods of managing IS security, AACSB: Analytical Thinking)

* 1. *Using your knowledge and intuition, describe why you think those differences occurred.*

Student responses will vary depending on the sources found by each team. (LO: 2, Learning Outcome: Describe different methods of managing IS security, AACSB: Analytical Thinking)

1. *Go to* www.accenture.com/us-en/insights/security/cost-cybercrime-study *and download Accenture’s 2019* Cost of Cybercrime Study *report (or a more recent report if one is available).*
2. *Summarize the survey with regard to safeguards and other measures that organizations use.*

The 2019 report documents that people-based attacks have increased the most. Therefore, several safeguards and measures are advised:

* Prioritize protecting people-based attacks: Countering internal threats is still one of the biggest challenges with a rise in phishing and ransomware attacks, as well as malicious insiders.
* Invest to limit information loss and business disruption: Already the most expensive consequence of cyberattacks, this is a growing concern with new privacy regulations such as GDPR and CCPA.
* Target technologies that reduce rising costs: Use automation, advanced analytics and security intelligence to manage the rising cost of discovering attacks, which is the largest component of spending. (LO: 2, Learning Outcome: Describe different methods of managing IS security, AACSB: Analytic Skills)

1. *Summarize the study’s conclusions with regard to the efficacy of organizational security measures.*

The 2019 report indicates that improving cybersecurity protection can decrease the cost of cybercrime and open up new revenue opportunities—a total value at risk of $US5.2 trillion globally over the next five years was calculated. Also, by prioritizing technologies that improve cybersecurity protection, organizations can reduce the consequences of cybercrime and unlock future economic value as higher levels of trust encourage more business from customers. (LO: 2, Learning Outcome: Describe different methods of managing IS security, AACSB: Analytic Skills)

1. *Does your team agree with the conclusions in the study? Explain your answer.*

Student responses may vary. (LO: 2, Learning Outcome: Describe different methods of managing IS security, AACSB: Analytic Skills)

1. *Suppose your boss asks for a summary of what your organization should do with regard to computer security. Using the knowledge of this chapter and your answer to the questions 10-4 through 10-6, create a PowerPoint presentation for your summary. Your presentation should include, but not be limited to:*
2. *Definition of key terms*
3. *Summary of threats*
4. *Summary of safeguards*
5. *Current trends in computer crime*
6. *What senior managers should do about computer security*
7. *What managers at all levels should do about computer security*

Student responses will vary. Look for the following important takeaway messages from this exercise:

* The median average cost of computer crime is increasing.
* Data loss is the principal cost of computer crime.
* People-focused attacks are on the rise.
* Security safeguards work.

(LO: 2, Learning Outcome: Describe different methods of managing IS security, AACSB: Written and Oral Communication)

|  |  |
| --- | --- |
| CASE STUDY 10 |  |

## Hitting the Target …

1. *Why did the attackers spear-phish a contractor to Target?*

Attackers look for any vulnerability they can find. Spear-phishing a contractor worked and gave them an entry point that was less noticeable than a direct attack on Target. (LO: 5, Learning Outcome: Describe different methods of managing IS security, AACSB: Analytical Thinking)

1. *Explain how a third-party contractor could weaken an organization’s overall security.*

As this example demonstrates, the contractor was vulnerable to spear-phishing and opened the door to these attackers on Target. Any third-party contractor can increase our vulnerability—so it is necessary to include them in our security programs. (LO: 5, Learning Outcome: Describe different methods of managing IS security, AACSB: Analytical Thinking)

1. *Describe how data was stolen from Target.*

Credentials were stolen from the contractor and used to break into a vendor server on Target’s network. Malware was introduced that found its way to the POS system, which then stole data from the POS terminals and directed the stolen data back to the criminals. (LO: 5, Learning Outcome: Describe different methods of managing IS security, AACSB: Analytical Thinking)

1. *How might a data loss at one organization affect other organizations?*

Many other organizations are affected, for example, a bank often must issue new bank cards after such an event. (LO: 5, Learning Outcome: Describe different methods of managing IS security, AACSB: Analytical Thinking)

1. *Explain why large organizations are attractive targets for attackers.*

Large organizations are obvious targets because if the attack is successful, the odds of substantial gain are greater. (LO: 5, Learning Outcome: Describe different methods of managing IS security, AACSB: Analytical Thinking)

1. *Why might chip-and-pin cards reduce this type of theft?*

Chip-and-pin cards prevent the cloning of credit/debit cards from stolen data. (LO: 5, Learning Outcome: Describe different methods of managing IS security, AACSB: Analytical Thinking)

1. *Why didn’t Target have a CISO before the data breach?*

Most organizations believe their security is being managed effectively until a breach occurs, then a security specialist such as a CISO is hired to place even more emphasis on the issue. In some cases, this may just be window-dressing for PR purposes, but could also be a sincere effort to make security measures more rigorous. (LO: 5, Learning Outcome: Describe different methods of managing IS security, AACSB: Analytical Thinking)

For an example illustrating the concepts found in this chapter, view the videos in [mymislab.com](http://mymislab.com/).