Course Learning Outcomes for Unit VI

Upon completion of this unit, students should be able to:

3. Examine the importance of mobile systems with regard to securing information and knowledge.
   3.1 Explore the importance of information systems (IS) security to organizations.
   3.2 Discuss sources of security threats to an organization.
   3.3 Explain safeguards for hardware and software components.

Course/Unit Learning Outcomes	Learning Activity
3.1	Unit Lesson Chapter 10 Unit VI PowerPoint Presentation
3.2	Unit Lesson Chapter 10 Unit VI PowerPoint Presentation
3.3	Unit Lesson Chapter 10 Unit VI PowerPoint Presentation

Reading Assignment

Chapter 10: Information Systems Security

Unit Lesson

Information Systems Security

Information systems (IS) security is important for keeping information available, confidential, and reliable. Through the use of access controls, unauthorized users can be prevented from accessing integral systems and potentially causing harm. An IS is vulnerable to threats that could potentially put organizational assets at risk. To protect this information, safeguards can be put in place to prevent theft or loss.

Security threats such as hacking have evolved into more sophisticated crimes of opportunities, such as illegally or maliciously deploying malware and ransomware. It used to be that hackers were the main source of threats, exploiting system vulnerabilities to prove a point. They were able to access the organization's information technology (IT) assets and, if they wanted to, compromise those assets. Today, malware and ransomware are a few of those threats and are often used by cyber-crime syndicates, large groups, or even corporations dedicated to performing rogue behavior with the purpose of fleecing legitimate organizations and individuals of cash and intellectual property. Other dangerous threats are minor cons (money mules and money launderers), hacktivists, intellectual theft and corporate espionage, and botnets (Kroenke & Boyle, 2017).

One recent example of a small-time botnet con was the arrest of malware kingpin Vladimir Tsastsin, who ran a click-fraud scheme for nearly 10 years and accumulated about $14 million dollars. The money was collected from unsuspecting victims using false advertising called click-fraud. The click-fraud scheme works when a malware-infected computer uses bots to pose as false entities that click on advertisements, tricking legitimate companies into thinking that people were viewing their advertisements on various websites. Vladimir would then collect pay-per-click monies from those unsuspecting companies (Andrew, 2017).

This type of scheme is not limited to just individuals but also to large organizations. In another example, a cyber-crime syndicate, which is called Operation GhostClick, infected a number of domain name servers (DNS) with malware called DNSChanger. This malware redirected requests through criminal-controlled servers, collecting money through fraudulent advertisement clicks from unsuspecting and legitimate companies (Lemos, 2011).

Threats are not always external; there are also internal threats. Internal threats usually come from within the organization. An example is when a disgruntled employee gains access to the system to cause harm. A second example is phishing. This occurs when an employee posts sensitive data to what he or she thinks is a legitimate company website or e-mail. Another example would be pre-texting; this is when someone pretends to be someone else for the purpose of gathering sensitive data such as social security numbers, passwords, and account information (Kroenke & Boyle, 2017).

So, what are organizations doing to prevent threats? Because of the changing nature of IS security, it is very difficult to predict threats, but when they occur, they can be mitigated through the implementation of safeguards. An example of a safeguard is the creation and use of strong passwords. Strong passwords contain a mixture of alphanumeric and special characters as well as lowercase and uppercase letters. Even though strong passwords are difficult to crack, they are vulnerable to brute-force attacks where a hacker tries every possible combination of characters to crack the password and gain entry. This is one way an individual can respond to security threats.

Organizations, on the other hand, must take a much more sophisticated approach. Organizations will need to develop and implement security policies; train employees about security risks; create an inventory of its IT assets, such as data and hardware; and evaluate potential risks to those assets. With this information, organizations can determine how much risk they are willing to accept and where security safeguards will need to be implemented (Kroenke & Boyle, 2017).

Integrated IS

The scenario at the beginning of Chapter 10 of the textbook in uCertify discusses some security concerns that can arise when integrating information systems. Let's take the company, Volkswagen, as an example. In their advertisements, Volkswagen uses an application (app) called Car-Net that will provide Internet access to music, GPS, diagnostics, and other apps from the vehicle's dash (Volkswagen, n.d.). So, what are the security risks if Internet access is provided in automobiles? Can cars with this technology create risk? Can hackers access Internet-capable cars and compromise them remotely? The answer is yes. Studies have shown that hackers have the ability to remotely access and sabotage the way a vehicle operates such as applying brakes to stop a car from moving, meddling with the stereo system, and controlling other vehicle functions without having to be anywhere near the car (Peterson, 2015; Rohrer & Hom, 2017; Vanian, 2016). This is possible because computers, or the controller area network (CAN), are used to control many of the car's operations (e.g., monitoring engine emissions, checking the airbag, sensing when fuel needs to be transferred from the tank to the engine). Self-driving cars are another example of how computers can control the operations of an automobile (Figure 1).

Figure 1: Self-driving car by Google
(U.S. Department of State, 2016)

Google is only one of several industries experimenting with self-driving cars. Today, we have several auto manufacturers of vehicles that already have some self-driving components such as auto-parking and anti-collision features. These features require the use of complex components such as computers and control modules. One of these features is what is known as self-parking, assisted parking, or autonomous parking, which is a self-maneuvering system that uses various sensors to move a vehicle from a traffic area into a parking space (e.g., parallel parking assistance) (Hamdan, 2017).

Despite the risks, having computers in just about every aspect of the automobile's operations has its benefits. By using computer modules and sensors to send data throughout the CAN, the vehicle has the ability to perform operations, such as self-diagnosing problems, detecting changes in engine temperature or voltage, detecting tire deflation, warning drivers when they are at risk of falling asleep, as well as other driving tasks, which are all intended to help improve the vehicle's reliability and safety (Pizzi, 2017).

Health IS

Another security concern is the potential for a person's health information to end up in the wrong hands. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is legislation that outlines how patients' medical information should be protected. The HIPAA law requires that all organizations that deal with patient health data to implement systems that comply with HIPAA rules. Failure to follow these rules to protect patient health information is a violation of the law (The Office of the National Coordinator for Health Information Technology, 2015).

Health information systems (HIS) have an important role in the privacy and security of health information. Patient health information can be secured through the use of certified electronic health records (EHR) that apply HIPAA rules. With the use of educational resources and tools, health providers and hospitals can mitigate privacy and security risks in their organizations. Why is it important to safeguard patient information? If patients cannot trust that their medical information is safe and secure, they may not be willing to disclose important health information. Withholding important and potentially life-saving information from healthcare practitioners can have drastic consequences such as loss of life (The Office of the National Coordinator for Health Information Technology, 2015).

Figure 2: The security of health records is an important piece in the information systems security puzzle.
(Baer, 2008)

Summary

Another security concern is what organizations do with client or customer data. If you fill out a form online, what happens to this data? Will the organization use it appropriately or sell it to spammers? This data can contain very personal information such as medical histories, credit card information, purchasing history, and financial information.

Data mining is when organizations collect customer data to help them better understand their customers' buying habits, to provide more personalized services, and to target potential customers. Technology has made it easier to collect and transmit data, whether it be a message or a bank account number. In this context, information has become a valuable commodity. Because of this, there can be tension between privacy and trust. We may be willing to give up some privacy by disclosing personal information to an organization, but we also want to know that we can trust that entity to protect that information (Kroenke & Boyle, 2017).

In this unit, we examined some information security threats and how organizations can mitigate these risks. Information security threats will continue to be complex and sophisticated, so we must remain vigilant in our response to those threats. As individuals, we can help by using strong passwords, attending security training sessions, following organizational security directives and guidelines, and reporting anything suspicious. For organizations, they must take a more systematic approach to security threats by addressing two critical security functions: developing and implementing an organization-wide security policy and managing risk.

References

Andrew, N. (2017). Is click fraud illegal or just unethical? Retrieved from https://ppcprotect.com/click-fraud-illegal/

Baer, R. (2008). *Doctor explains x-ray to patient* [Image]. Retrieved from https://commons.wikimedia.org/wiki/File:Doctor_explains_x-ray_to_patient.jpg

Hamdan, L. (2017, November 13). Revealed: How Ford is gearing up for tomorrow land. *Arabianbusiness.com.* Retrieved from https://search-proquest-com.libraryresources.columbiasouthern.edu/docview/1963302512?accountid=33337

Kroenke, D. M., & Boyle, R. J. (2017). *Using MIS* (10th ed.). New York, NY: Pearson.

Lemos, R. (2011). As cybercrimes go international, so must enforcement agencies. Retrieved from https://www.infoworld.com/article/2621345/cyber-crime/as-cyber-crimes-go-international--so-must-enforcement-agencies.html

The Office of the National Coordinator for Health Information Technology. (2015, April). *Guide to privacy and security of electronic health information*. Retrieved from https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Peterson, A. (2015, August 14). Here is how you learn to hack a car. *Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2015/08/14/here-is-how-you-learn-to-hack-a-car/

Pizzi, P. J. (2017). Connected cars and automated driving: Privacy challenges on wheels. *Defense Counsel Journal, 84*(3), 1–14. Retrieved from https://search-proquest-com.libraryresources.columbiasouthern.edu/docview/1924515502?accountid=33337

Rohrer, K. K., & Hom, N. S. (2017). Who's responsible for cybersecurity? *Strategic Finance, 99*(4), 62–63. Retrieved from https://search-proquest-com.libraryresources.columbiasouthern.edu/docview/1947781911?accountid=33337

U.S. Department of State. (2016). *Secretary Kerry views the computers inside one of Google's self-driving cars at the 2016 global entrepreneurship summit's innovation marketplace at Stanford University* [Image]. Retrieved from https://commons.wikimedia.org/w/index.php?curid=49674725

Vanian, J. (2016, January 26). Security experts say that hacking cars is easy. *Fortune*. Retrieved from http://fortune.com/2016/01/26/security-experts-hack-cars/

Volkswagen. (n.d.). Volkswagen car-net. Retrieved from http://www.vwcarnetconnect.com/

Suggested Reading

The following chapters are located in the textbook in uCertify. Chapter 4 is a review of material presented previously, but you may find the information to be helpful as you complete this unit's assignment. Chapter 7 focuses on security within the workplace.

Chapter 4: Hardware, Software, and Mobile Systems, Q4-7

Chapter 7: Security Guide

In order to access the following resources, click the links below:

It happens all the time; an employee with proprietary knowledge leaves a company with that knowledge. What does the company do? This article explores that question.

Richmond, R., Morrison, K. M., & Lim, E. (2017). What do you do when an employee with access to your company's trade secrets leaves to work for a competitor? *Employee Relations Law Journal, 43*(2), 36–44. Retrieved from https://libraryresources.columbiasouthern.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=124285832&site=ehost-live&scope=site

More and more workplaces are turning to mobile solutions. However, these solutions come with their own issues. The article below examines the different obstacles that organizations face when converting to a more digital workplace.

Vieraitis, B. (2003). 5 hurdles to mobile and wireless deployments ... and how to overcome them: Today's work force is demanding mobile, flexible, and real-time access to critical data. But, you're bound to encounter a few potholes along the road to anytime-anywhere computing. *Mobile Business Advisor*, *21*(5), 20. Retrieved from http://link.galegroup.com.libraryresources.columbiasouthern.edu/apps/doc/A110026621/CDB?u=oran95108&sid=CDB&xid=00b6246b

Learning Activities (Nongraded)

Nongraded Learning Activities are provided to aid students in their course of study. You do not have to submit them. If you have questions, contact your instructor for further guidance and information.

To test your knowledge of the material covered in this unit, complete the activities listed below.

- Chapter 10 Active Review
- Chapter 10 Using Your Knowledge
- Chapter 10 Collaboration Exercise
- Chapter 10 Review Questions
- Chapter 10 Cards

The activities are located within the chapter readings in uCertify. The Chapter 10 Active Review, Using Your Knowledge, Collaboration Exercise, and Review Questions are located at the end of the chapter. The cards can be accessed by clicking on the Cards icon within uCertify, which is located to the right of the chapter title, and the icon in uCertify resembles the image shown below.