LESSON PREVIEW

Methods of Securing Information

Cybersecurity is one of the most important aspects of a business in today's world. Businesses maintain a great deal of data, much of which is sensitive to both the inner workings of the business and the customers. Not only are there risks from cybercriminals but also from unavoidable natural disasters.

There are many ways that cybercriminals can attack a system, from inside and outside. This module covers most of the types of cyberattacks that originate from infiltrating hardware and software as well as those attacks by people who target employees and get them to divulge confidential information.

No system can be completely safe all the time but companies must use all the resources at their disposal to protect their systems and data and to mitigate the risks associated with cyberattack.

After completing this section, you will be able to:

- Define cybercrime.
- Define cyberattack.
- Describe state-sponsored cyberwarfare.
- Explain how computer systems and data are protected from natural disasters.
- Define what white hat hackers are and how they are used by organizations.
- Describe what black hat hackers do.
- Define malware.
- Describe computer viruses and how to recognize an infection.
- Describe the following methods of cyberattacks: Trojan horse, ransomware, keystroke loggers, packet sniffers, DoS and DDoS, and rootkits.
- Describe the impact of these forms of cyberattacks on MIS.
- Describe phishing, spear phishing, and social engineering.
- Describe how cybersercurity teams assess and mitigate risks to computer networks.
- Describe firewalls and how they are used to protect data.
- Describe how behavioral science protects data security systems.
- Describe how backups protect data.

NOTES

Cybercrime

Cybercrime is a crime in which a computer is the object of the crime or is used to commit a crime or offense. Cybercrimes can be committed by highly skilled individuals or by novice hackers. The two main types of cybercrimes are single-event and ongoing series-of-events attacks.

Single-event cybercrimes occur when victims endure a single event such as downloading a Trojan horse virus, installing a keystroke logger, or falling victim to identity theft and/or e-commerce fraud.

Ongoing series-of-events cybercrimes are more serious and include cyberstalking, child predation, extortion, blackmail, and terrorist activities.

NOTES

Cyberattack

A **cyberattack** is a deliberate misuse of computers and networks via the Internet. Cyberattacks use malicious code to modify the normal operations of a computer or network. One type of cyberattack aims to disable a target computer or prevent it from accessing a network or the Internet. The second type of attack is designed to gain access to data stored on a device or to gain administrative privileges to a device.

Cyberattacks include the following: pharming and phishing, spamming and spoofing, spyware, Trojans and viruses, identity and information theft, and denial of service (DoS) attacks.

NOTES

State-Sponsored Cyberwarfare

State-sponsored cyberwarfare is defined as cyberattacks that originate and are executed by foreign governments. Cyberwarfare attacks are relatively inexpensive when compared to traditional warfare, difficult to trace and identify, and can cause widespread damage to IT infrastructure. Cyberwarfare can be utilized to send warnings, to intentionally harm resources, or to create conflict between countries.

NOTES

Protecting Computer Systems and Data from Natural Disasters

Regardless of where a business operates, it is at risk for a **natural disaster**, which may take the form of wildfires, floods, hurricanes, tornados, and earthquakes. Businesses need to take steps to protect computer systems, data, and information from natural disasters.

Four steps to help protect businesses from natural disasters are:

- Business continuity plan
- Use of offsite Cloud storage
- Maintenance of data inventory
- Geographic data redundancy

Businesses often store data in a variety of places and should know the location of where all of their data are stored. This can help businesses retrieve and locate data. It is also valuable to replicate and store data in separate locations.

NOTES

White Hat Hackers

White hat hackers are nonmalicious computer security experts who test the security measures of an organization's information systems to ensure they are protected against malicious intrusions. Some of the tasks they perform include **penetration testing**, **vulnerability testing**, and testing of in-place security systems. White hat hackers are often hired as consultants to expose weaknesses in a network's firewalls.

White hat hackers use the same techniques and tools that are used by illegitimate hackers, but today's white hat hackers utilize a new type of technology to test security. Breach and attack simulation technologies are used to automate hacking and threat/infiltration analysis.

While white hat hacking can be very effective, it can be very expensive, which makes it difficult for some companies to utilize these experts.

There are a variety of college cybersecurity programs that focus on ethical/white hat hacking. You can take college courses in this area and eventually work in this career field.

NOTES

Black Hat Hackers

Black hat hackers break into computer systems with the intent of causing damage or stealing data. Most black hat hackers learned how to hack computers and systems using scripts that are available on the Internet. Novice hackers are often referred to as script kiddies.

Black hat malware kits are available for purchase on the Dark Web. The Dark Web is content posted on the Internet that is not indexed by popular search engines such as Google. To access the Dark Web, a specific web browser is required. One of the most popular search engines used to access the Dark Web is Tor.

NOTES

Malware

Malware is designed to steal information, destroy data, impact the operations of a computer or network, or frustrate the user. Malware programs are often developed by hackers or teams of hackers who are looking to make money by launching the malware on their own or by selling it on the Dark Web. Malware can be used for a variety of purposes, including cyberextortion, cyberterrorism, protest, or cyberstalking.

NOTES

Computer Viruses

A **computer virus** is software that infects computers and is created using computer code. Viruses can destroy programs or alter the operations of a computer or network. There are many symptoms your computer may exhibit when it has been infected with a virus. Some of these are:

- The operating system may not launch properly and the user may need to reboot and restart the computer frequently to ensure all programs are starting and working fine.
- Critical files may get deleted automatically; this can happen periodically or all at once.
- Error messages will become prevalent; it may become difficult to save documents, and the computer may run slower than usual. If a system or network is infected severely, it may black out or not even launch the start-up process.

A computer virus works much the same as a biological virus. A biological virus is spread from host to host and the virus has the ability to replicate itself. A computer virus attacks a digital device using a series of actions and also has the ability to replicate itself.

- The virus arrives via email attachment, file download, or by visiting a website that has been infected.
- An action such as running or opening a file activates the virus.
- Once activated, the virus copies itself into files and other locations on your computer.
- Next, the infection spreads to other computers via infected email, files, or contact with infected websites.
- Finally, the payload or the component of a virus that executes the malicious activity hits the computer and other infected devices.
- These actions are repeated over and over, resulting in a full-blown virus attack.

Viruses not only attack laptops and desktops but can also attack mobile devices, including smartphones and tablet computers.

NOTES

Trojan Horses

A **Trojan**, sometimes called a **Trojan horse**, is a program that appears legitimate but executes an unwanted activity when activated. Trojans are often used to install key loggers or packet sniffers that can find passwords, destroy data, or bypass firewalls. Trojans are similar to viruses, but do not replicate themselves and are commonly found attached to free downloads and apps.

Trojans are designed using some sort of social engineering tactic that tricks the users into loading and executing the Trojan. Once the Trojan has been deployed, hackers have the ability create a backdoor to the user's system, which allows them to spy on computer activities and steal sensitive data. Many Trojans are designed to give hackers the ability to delete, block, modify, and copy data. Trojans can also be used to interrupt network communication and to negatively affect computer performance.

NOTES

Ransomware

Ransomware is malware that makes a computer's data inaccessible until a ransom is paid. It usually invades a computer in a Trojan horse, in a legitimate-looking email, or with a worm in a networked computer. Ransomware typically encrypts the victim's data files and offers to decrypt the files for a ransom payment. Another version of ransomware threatens to make the victim's personal files public unless the ransom is paid.

One of the most popular methods used in ransomware attacks is through phishing, commonly executed through email messages. Illegitimate file attachments are included in what appears to be a legitimate email message. Once the illegitimate file is downloaded and opened, the ransomware can take over the computer.

NOTES

Keystroke Loggers, Packet Sniffers, and Rootkits

A **keystroke logger** is a form of spyware that records all actions typed on a keyboard. It may consist of hardware devices and/or software applications. Newer forms of keystroke loggers are Cloud based and are available for use by parents, organizations, and others to record most computer activities that take place via a web browser, including gaming, chatting, and website visits.

Packet sniffers (or packet analyzers) are specialized hardware or software that capture packets transmitted over a network. Packet sniffers record the data packets as they are sent over a network and copy the information to a designated file. This process is known as packet capture. Legitimate sniffers are used for routine examination and problem detection. Unauthorized sniffers are used to steal information.

A **rootkit** is a type of malicious computer program that is designed to allow unauthorized access to cybercriminals who then can control that computer remotely. Rootkits are used to steal passwords and credit card and banking information. While security software often can catch and disable a rootkit when it has been installed, some rootkits go undetected for long periods of time. When this occurs, often the only remedy is to uninstall the computer's operating system and then reload it.

NOTES

Denial of Service Attacks

A **Denial of Service** (**DoS**) attack occurs on a network that is designed to interrupt or stop network traffic by flooding it with too many requests. A DoS attack is carried out by one device, whereas a Distributed Denial of Service (DDoS) attack uses many devices to slow down or crash a network. Once the computers are infected, they act as **zombies** (**bots**) and work together to send messages and site requests, thus creating huge volumes of network traffic that result in a network crash.

A DoS attack takes place when a hacker uses software to infect devices, including laptops, desktops, tablets, and Internet of Things (IoT) devices, turning each into a zombie. A group of computers under the control of a hacker is referred to as a **botnet**. When a botnet has been established, the hacker is able to direct each device via remote access. For example, when an IP address is targeted by a botnet, each zombie computer will simultaneously send requests to that IP address, which then can potentially cause the targeted server to slow down or even shut down, resulting in a DoS.

NOTES

How Packet Sniffers, Rootkits, and DoS Attacks Affect Management Information Systems

Packet sniffers, rootkits, and DoS attacks can cause financial losses, lost productivity, and downtime. It is important that the risk of these threats be analyzed by an organization and that proper plans for monitoring, detection, and remediation are in place. The following statistics were compiled in 2019 to show the impact of different malware and network attacks:

- 43% of all cyberattacks are aimed at small businesses.
- 91% of attacks launch with a phishing email.
- 85% of all attachments emailed daily are harmful for their intended recipients.
- 38% of malicious attachments are masked as one Microsoft Office type of file or another.

NOTES

Phishing and Spear Phishing

Phishing is the illegitimate use of an email message that appears to be from an established organization such as a bank, financial institution, or insurance company. The message often contains the company's logo and identifying information and uses legitimate looking email messages to con a user into giving up private information such as account numbers, social security numbers, and personal information.

Spear phishing is a type of email scam that is directed toward a specific person or organization, unlike phishing, which does not have a specific target. Spear phishing attacks are designed to steal data, and some attacks may be designed to install malicious software on a device.

Spear phishing may work like this: An email arrives in your inbox and appears to be from the bank where you got your car loan. You open the message, which prompts you to visit a bogus site that appears to be your bank. You fail to identify the site as bogus and enter your username and password to access your account. This information is recorded and can now be used by the attacker.

NOTES

Measures Taken to Assess Risks and Protect Data Systems

Cybersecurity personnel use a **cybersecurity risk assessment** to ensure data and systems are protected. The primary purposes of this are to inform decision-makers and to support proper risk responses.

Risk can be calculated using the following calculation: Risk = Threat × Vulnerability × Asset. The process attempts to answer the following questions:

- What are our organization's most important information technology assets?
- What data breach would have a major impact on our business?
- What are the relevant threats and the threat sources to our organization?
- What are the internal and external vulnerabilities?
- What is the impact if those vulnerabilities are exploited?
- What is the likelihood of exploitation?
- What incidents could impact the ability of the business to function?
- What is the level of risk our organization is comfortable taking?

NOTES

Assessing and Mitigating Risks to Computers and Computer Networks

Once a cybersecurity risk assessment has been conducted and the various questions in the risk assessment have been answered, an organization will be able to decide what to protect. IT security controls can be investigated and developed and then data security strategies to mitigate risk can be employed. Before that can occur, the following questions must be answered:

- What is the risk I am reducing?
- Is this the highest priority security risk?
- Am I reducing the risk in the most cost-effective way?

After these questions have been answered, an organization can begin the process of determining the best policies and procedures for threat mitigation.

NOTES

Firewalls

A **firewall** is hardware or software used to keep a computer secure from outside threats. They allow or block Internet traffic in and out of a network or computer. The most ideal firewall configuration consists of both hardware and software.

Firewalls are designed for small, medium, and large businesses. Many firms opt to have their firewalls created and maintained by outside firms.

Since Cloud systems are not part of an organization's internal network, they are often not protected by a network firewall. Therefore companies that use Cloud-based file sharing services may require the use of a dedicated firewall for Cloud sharing.

Large organizations often utilize a system of complex firewalls to protect their networks. These firewalls can be configured to prevent unauthorized access to networks from outside the organization and to prevent employees from sending or transmitting sensitive data.

NOTES

Social Engineering

Social engineering is the use of computers and digital technology to manipulate people so they divulge confidential information or to gain unauthorized access to a digital device so malware can be installed. Social engineering is popular because it is often easier to exploit an individual's trusting nature than it is to hack a system or develop malicious software.

To avoid falling victim to a social engineering attack you should:

- Research the facts and sites contained in an email message or phone call.
- Slow down to think about the scenario.
- Be mindful of web searches to make sure you are landing on legitimate sites.

NOTES

Using Behavioral Science

Traditional methods of securing networks and systems (including firewalls, two-factor authentication, and passwords) are no longer enough to ensure data and system security. Organizations now use **behavior science** to deal with the increase in cybersecurity threats and the decrease in the effectiveness of traditional security in their data and network security policies.

User and entity behavior analytics (UEBA) is a type of cybersecurity that observes and records the conduct of computer and network users, both inside and outside the organization. This information is used to identify any behavior that deviates from normal behavior.

NOTES

How MIS Uses Backups to Protect Data

Backup and recovery (also referred to as operational recovery) are important components in the overall MIS and IT plan. This is the process of generating and storing duplicates of data sets to help prevent against data loss should an issue occur.

Data backups often are stored offsite on company-owned servers or servers owned by another organization. Cloud backup is fast becoming the backup method of choice for many organizations. It utilizes an outside organization's servers to store information via the Cloud.

Data backup is critical because, in the event of primary data failure, data can be restored from an earlier point in time. Data backup should occur at regular intervals to minimize the amount of data that could potentially be lost. The more time in between backups, the greater significant data can be lost.

NOTES

Design element: Vector abstract geometric background; -strizh-/Getty Images