

Principles of Management Information Systems

Lecture 10

MGM331

Cybercrime and Information System Security

Prepared by
Dr. Eng. Youssef Ntefeh

Lecture 10

- The security of data and information systems used in business is of utmost importance.
- Confidential business data and private customer and employee information must be safeguarded, and systems must be protected against malicious acts of theft or disruption.
- Although the need for security is obvious, it must often be balanced against other business needs.

Lecture 10

- Business managers, IS professionals, and IS users all face a number of complex trade-offs regarding IS security, such as the following:
 - ❑ How much effort and money should be spent to safeguard against computer crime? (In other words, how safe is safe enough?)
 - ❑ What should be done if recommended computer security safeguards make conducting business more difficult for customers and employees, resulting in lost sales and increased costs?
 - ❑ If a firm is a victim of a computer crime, should it pursue the criminals at all costs, maintain a low profile to avoid the negative publicity, inform affected customers, or take some other action?

Principles

- ✓ Computer crime is a serious and rapidly growing area of concern requiring management attention.
- ✓ Organizations must take strong measures to ensure secure, private, and reliable computing experiences for their employees, customers, and business partners.

Learning Objectives

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

Lecture 10: Cybercrime and Information System Security

The Threat Landscape

Implementing Secure, Private, Reliable Computing

Why Computer Incidents Are So Prevalent

Types of Exploits

Ransomware
Viruses
Worms
Trojan Horses
Spam
DDoS attack
Phishing
Identity Theft

Risk Assessment

Establishing a Security Policy

Educating Employees

Prevention

Detection

Response

Computer Forensics

The Threat Landscape

- The number of cybercrimes being committed against individuals, organizations, and governments continues to increase, and the destructive impact of these crimes is also intensifying.
- The brands, reputation, and earnings of many organizations around the world have been negatively impacted by such crimes.
- As a result, organizations are putting in place a range of countermeasures to combat cybercrime. For instance, the worldwide financial services industry spent \$27.4 billion on IT security and fraud prevention in 2015.

The Threat Landscape

- And a recent survey of more than 10,000 IT professionals around the world revealed the following:
 - ❑ 58 percent of global companies have an overall security strategy.
 - ❑ 54 percent have a CISO (chief information security officer) in charge of security.
 - ❑ 53 percent have employee security awareness and training programs.
 - ❑ 52 percent have security standards for third parties.
 - ❑ 49 percent conduct threat assessments.
 - ❑ 48 percent actively monitor and analyze security intelligence.

Why Computer Incidents Are So Prevalent

- Increasing computing complexity, higher computer user expectations, expanding and changing systems, an increase in the prevalence of bring your own device (BYOD) policies, a growing reliance on software with known vulnerabilities, and the increasing sophistication of those who would do harm have caused a dramatic increase in the number, variety, and severity of security incidents are increasing dramatically.

Why Computer Incidents Are So Prevalent

Increasing Complexity Increases Vulnerability

- The computing environment has become enormously complex.
- Cloud computing, networks, computers, mobile devices, virtualization, operating systems applications, Web sites, switches, routers, and gateways are interconnected and driven by hundreds of millions of lines of code.
- This environment continues to increase in complexity every day. The number of possible entry points to a network expands continually as more devices are added, increasing the possibility of security breaches.

Why Computer Incidents Are So Prevalent

Higher Computer User Expectations

- Today, time means money, and the faster computer users can solve a problem, the sooner they can be productive. As a result, computer help desks are under intense pressure to respond very quickly to users' questions.
- Under duress, help desk personnel sometimes forget to verify users' identities or to check whether they are authorized to perform a requested action.
- In addition, even though most have been warned against doing so, some computer users share their login ID and password with other coworkers who have forgotten their own passwords. This can enable workers to gain access to information systems and data for which they are not authorized.

Why Computer Incidents Are So Prevalent

Expanding and Changing Systems Introduce New Risks

- Business has moved from an era of stand-alone computers, in which critical data was stored on an isolated mainframe computer in a locked room, to an era in which personal computers and mobile devices connect to networks with millions of other computers, all capable of sharing information.
- Businesses have moved quickly into e-commerce, mobile computing, collaborative work groups, global business, and interorganizational information systems. Information technology has become a necessary tool for organizations to achieve their goals.
- However, it is increasingly difficult for IT organizations to keep up with the pace of technological change, successfully perform an ongoing assessment of new security risks, and implement approaches for dealing with them.

Why Computer Incidents Are So Prevalent

Increased Prevalence of Bring Your Own Device Policies

- Bring your own device (BYOD) is a business policy that permits, and in some cases encourages, employees to use their own mobile devices (smartphones, tablets, or laptops) to access company computing resources and applications, including email, corporate databases, the corporate intranet, and the Internet.
- Proponents of BYOD say it improves employee productivity by allowing workers to use devices with which they are already familiar—while also helping to create an image of a company as a flexible and progressive employer.

Why Computer Incidents Are So Prevalent

- Most companies have found they cannot entirely prevent employees from using their own devices to perform work functions.
- However, this practice raises many potential security issues as it is highly likely that such devices are also used for nonwork activity (browsing Web sites, blogging, shopping, visiting social networks, etc.) that exposes them to malware much more frequently than a device used strictly for business purposes. That malware may then be spread throughout the company.
- In addition, BYOD makes it extremely difficult for IT organizations to safeguard additional portable devices with various operating systems and a myriad of applications.

Why Computer Incidents Are So Prevalent

Growing Reliance on Commercial Software with Known Vulnerabilities

- In computing, an exploit is an attack on an information system that takes advantage of a particular system vulnerability.
- Often this attack is due to poor system design or implementation. Once the vulnerability is discovered, software developers create and issue a “fix,” or patch, to eliminate the problem.
- Users of the system or application are responsible for obtaining and installing the patch, which they can usually download from the Web. (These fixes are in addition to other maintenance and project work that software developers perform.)

Why Computer Incidents Are So Prevalent

- Any delay in installing a patch exposes the user to a potential security breach. The need to install a fix to prevent a hacker from taking advantage of a known system vulnerability can create a time management dilemma for system support personnel trying to balance a busy work schedule.
- Should they install a patch that, if left uninstalled, could lead to a security breach, or should they complete assigned project work so that the anticipated project savings and benefits from the project can begin to accrue on schedule?
- According to Secunia, a provider of vulnerability intelligence and management tools, the number of new software vulnerabilities identified in 2014 jumped 18 percent from the previous year to 15,435—an average of 42 per day

Why Computer Incidents Are So Prevalent

Increasing Sophistication of Those Who Would Do Harm

- Previously, the stereotype of a computer troublemaker was that of an introverted “geek” working on his own and motivated by the desire to gain some degree of notoriety.
- This individual was armed with specialized, but limited, knowledge of computers and networks and used rudimentary tools, perhaps downloaded from the Internet, to execute his exploits.
- While such individuals still exist, it is not this stereotyped individual who is the biggest threat to IT security. Today’s computer menace is much better organized and may be part of an organized group that has an agenda and targets specific organizations and Web sites.

Why Computer Incidents Are So Prevalent

- Some of these groups have ample resources, including money and sophisticated tools to support their efforts.
- Today's computer attacker has greater depth of knowledge and expertise in getting around computer and network security safeguards.
- Table 13.2 summarizes the types of perpetrators of computer mischief, crime, and damage.

Why Computer Incidents Are So Prevalent

Type of Perpetrator	Description
Black hat hacker	Someone who violates computer or Internet security maliciously or for illegal personal gain (in contrast to a white hat hacker who is someone who has been hired by an organization to test the security of its information systems)
Cracker	An individual who causes problems, steals data, and corrupts systems
Malicious insider	An employee or contractor who attempts to gain financially and/or disrupt a company's information systems and business operations
Industrial spy	An individual who captures trade secrets and attempts to gain an unfair competitive advantage
Cybercriminal	Someone who attacks a computer system or network for financial gain
Hacktivist	An individual who hacks computers or Web sites in an attempt to promote a political ideology
Cyberterrorist	Someone who attempts to destroy the infrastructure components of governments, financial institutions, and other corporations, utilities, and emergency response units

Lecture 10: Cybercrime and Information System Security

The Threat Landscape

Implementing Secure, Private, Reliable Computing

Why Computer Incidents Are So Prevalent

Types of Exploits

Ransomware
Viruses
Worms
Trojan Horses
Spam
DDoS attack
Phishing
Identity Theft

Risk Assessment

Establishing a Security Policy

Educating Employees

Prevention

Detection

Response

Computer Forensics

Types of Exploits

- There are numerous types of computer attacks, with new varieties being invented all the time. This section discusses some of the more common attacks, including ransomware, viruses, worms, Trojan horses, spam, distributed denial-of-service, phishing, identity theft, and cyberespionage.

Types of Exploits

- While we usually think of such exploits being aimed at computers, smartphones continue to become more computer capable. Increasingly, smartphone users store an array of personal identity information on their devices, including credit card numbers and bank account numbers.
- The more people use their smartphones for these purposes, the more attractive these devices become as targets for cyber thieves.

DIFFERENCE BETWEEN

Viruses

Malware

Trojans

Ransomware

Spyware

& Worms!

Types of Exploits

Viruses

- Computer virus has become an umbrella term for many types of malicious code. Technically, a *virus* is a piece of programming code, usually disguised as something else, that causes a computer to behave in an unexpected and usually undesirable manner.
- For example, the virus may be programmed to display a certain message on the computer's display screen, delete or modify a certain document, or reformat the hard drive.
- Almost all viruses are attached to a file, so that only when the infected file is opened, the virus executes. A virus is spread to other machines when a computer user shares an infected file or sends an email with a virus-infected attachment. In other words, viruses spread by the action of the "infected" computer user.

Types of Exploits

Trojan Horses

- A *Trojan horse* is a seemingly harmless program in which malicious code is hidden. A victim on the receiving end of a Trojan horse is usually tricked into opening it because it appears to be useful software from a legitimate source, such as an update for software the user currently has installed on his or her computer.
- The program's harmful payload might be designed to enable the hacker to destroy hard drives, corrupt files, control the computer remotely, launch attacks against other computers, steal passwords or spy on users by recording keystrokes and transmitting them to a server operated by a third party.
- A Trojan horse often creates a “backdoor” on a computer that enables an attacker to gain future access to the system and compromise confidential or private information.

Types of Exploits

Ransomware

- *Ransomware* is malware that stops you from using your computer or accessing your data until you meet certain demands such as paying a ransom or sending information to the attacker.
- Computers become infected when users open an email attachment containing the malware or are lured to a compromised Web site by a deceptive email or pop-up window.

Types of Exploits

Worms

- Unlike a computer virus, which requires users to spread infected files to other users, a *worm* is a harmful program that resides in the active memory of the computer and duplicates itself.
- Worms differ from viruses in that they can propagate without human intervention, often sending copies of themselves to other computers by email.
- A worm is capable of replicating itself on your computer so that it can potentially send out thousands of copies of itself to everyone in your email address book, for example.

Types of Exploits

Spam

- Email **spam** is the use of email systems to send unwanted email to large numbers of people.
- Most spam is a form of low-cost commercial advertising, sometimes for questionable products such as phony get-rich-quick schemes and worthless stock.
- Spam is also an extremely inexpensive method of marketing used by many legitimate organizations. For example, a company might send email to a broad cross section of potential customers to announce the release of a new product in an attempt to increase initial sales. However, spam is also used to deliver harmful worms and other malware.

Types of Exploits

Spam

- Many companies—including Google, Microsoft, and Yahoo offer free email services. Spammers often seek to use email accounts from such major, free, and reputable Web-based email service providers, as their spam can be sent at no charge and is less likely to be blocked.
- Spammers can defeat the registration process of the free email services by launching a coordinated bot attack that can sign up for thousands of email accounts. These accounts are then used by the spammers to send thousands of untraceable email messages for free.
- A partial solution to this problem is the use of CAPTCHA to ensure that only humans obtain free accounts.
- **CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart)** software generates and grades tests that humans can pass and all but the most sophisticated computer programs cannot.

Types of Exploits

Distributed Denial-of-Service Attacks

- A *distributed denial-of-service (DDoS) attack* is one in which a malicious hacker takes over computers via the Internet and causes them to flood a target site with demands for data and other small tasks.
- A distributed denial of service attack does not involve infiltration of the targeted system. Instead, it keeps the target so busy responding to a stream of automated requests that legitimate users cannot get in

Types of Exploits

• Distributed Denial-of-Service Attacks

1. Hacker's computer sends several simultaneous requests; each request asks to establish a connection to the server but supplies false return information. In a distributed DoS attack, multiple computers send multiple requests at one time.

Hello? I'd like some info...

2. The server tries to respond to each request but can't locate the computer because false return information was provided. The server waits for a short period of time before closing the connection, which ties up the server and keeps others from connecting.

I can't find you, I'll wait and try again...

3. The hacker's computer continues to send new requests so, as a connection is closed by the server, a new request is waiting. This cycle continues, which ties up the server indefinitely.

Hello? I'd like some info...



HACKER'S COMPUTER



WEB SERVER

Hello? I'd like some info...

I'm busy, I can't help you right now.



LEGITIMATE COMPUTER

4. The server becomes so overwhelmed that legitimate requests cannot get through and, eventually, the server usually crashes.



Types of Exploits

- The term *botnet* is used to describe a large group of computers, which are controlled from one or more remote locations by hackers, without the knowledge or consent of their owners.
- The collective processing capacity of some botnets exceeds that of the world's most powerful supercomputers.
- Based on a command by the attacker or at a preset time, the botnet computers (called zombies) go into action, each sending a simple request for access to the target site again and again dozens of times per second.
- The target computers become so overwhelmed by requests for service that legitimate users are unable to get through to the target computer.

Types of Exploits

Phishing

- *Phishing* is the act of fraudulently using email to try to get the recipient to reveal personal data.
- In a phishing scam, con artists send legitimate-looking emails urging the recipient to take action to avoid a negative consequence or to receive a reward.
- The requested action may involve clicking on a link to a Web site or opening an email attachment. These emails lead consumers to counterfeit Web sites designed to trick them into divulging personal data or to download malware onto their computers.

Types of Exploits

Identity Theft

- *Identity theft* is the theft of personal information, which is then used without the owner's permission.
- Often, stolen personal identification information, such as a person's name, Social Security number, or credit card number, is used to commit fraud or other crimes. Thieves may use a consumer's credit card number to charge items to that person's account, use identification information to apply for a new credit card or a loan in a consumer's name, or use a consumer's name and Social Security number to receive government benefits.
- Thieves also often sell personal identification information on the black market.
- A *data breach* is the unintended release of sensitive data or the access of sensitive data by unauthorized individuals, often resulting in identify theft.

Types of Exploits

Cyberespionage

- *Cyberespionage* involves the deployment of malware that secretly steals data in the computer systems of organizations, such as government agencies, military contractors, political organizations, and manufacturing firms.
- The type of data most frequently targeted includes data that can provide an unfair competitive advantage to the perpetrator. This data is typically not public knowledge and may even be protected via patent, copyright, or trade secret. High value data includes the following:
 - ☐ Sales, marketing, and new product development plans, schedules, and budgets
 - ☐ Details about product designs and innovative processes
 - ☐ Employee personal information
 - ☐ Customer and client data
 - ☐ Sensitive information about partners and partner agreements

Lecture 10: Cybercrime and Information System Security

The Threat Landscape

Implementing Secure, Private, Reliable Computing

Why Computer Incidents Are So Prevalent

Types of Exploits

Ransomware
Viruses
Worms
Trojan Horses
Spam
DDoS attack
Phishing
Identity Theft

Risk Assessment

Establishing a Security Policy

Educating Employees

Prevention

Detection

Response

Computer Forensics

Implementing Secure, Private, Reliable Computing

- Organizations worldwide are increasingly demanding methods of computing that deliver secure, private, and reliable computing experiences based on sound business practices.
- Software and hardware manufacturers, consultants, and system designers and developers all understand that this is a priority for their customers.
- A strong security program begins by assessing threats to the organization's computers and network, identifying actions that address the most serious vulnerabilities, and educating end users about the risks involved and the actions they must take to prevent a security incident.

Implementing Secure, Private, Reliable Computing

- An organization's IS security group must lead the effort to prevent security breaches by implementing security policies and procedures, as well as effectively employing available hardware and software tools.
- However, no security system is perfect, so systems and procedures must be monitored to detect a possible intrusion. If an intrusion occurs, there must be a clear reaction plan that addresses notification, evidence protection, activity log maintenance, containment, eradication, and recovery.

Implementing Secure, Private, Reliable Computing

Risk Assessment

- *Risk assessment* is the process of assessing security-related risks to an organization's computers and networks from both internal and external threats.
- Such threats can prevent an organization from meeting its key business objectives.
- The goal of risk assessment is to identify which investments of time and resources will best protect the organization from its most likely and serious threats.

Implementing Secure, Private, Reliable Computing

Establishing a Security Policy

- A *security policy* defines an organization's security requirements, as well as the controls and sanctions needed to meet those requirements.
- A good security policy delineates responsibilities and the behavior expected of members of the organization.
- A security policy outlines *what* needs to be done but not *how* to do it.
- The details of *how* to accomplish the goals of the policy are typically provided in separate documents and procedure guidelines.

Implementing Secure, Private, Reliable Computing

Educating Employees and Contract Workers

- Creating and enhancing user awareness of security policies is an ongoing security priority for companies.
- Employees and contract workers must be educated about the importance of security so that they will be motivated to understand and follow security policies.
- This can often be accomplished by discussing recent security incidents that affected the organization.
- Users must understand that they are a key part of the security system and that they have certain responsibilities.

Implementing Secure, Private, Reliable Computing

- For example, users must help protect an organization's information systems and data by doing the following:
 - ❑ Guarding their passwords to protect against unauthorized access to their accounts.
 - ❑ Prohibiting others from using their passwords.
 - ❑ Applying strict access controls (file and directory permissions) to protect data from disclosure or destruction.
 - ❑ Reporting all unusual activity to the organization's IT security group.

Implementing Secure, Private, Reliable Computing

Simple self-assessment security test that employees should be asked to complete.

- Do you have the most current version of your operating system installed?
- Do you have the most current version of firewall, antivirus, and malware software installed?
- Do you install updates to all your software when you receive notice that a new update is available?
- Do you use different, strong passwords for each of your accounts and applications—a minimum of 10 characters with a mix of capital and lower case letters, numbers, and special characters?
- Are you familiar with and do you follow your organization's policies in regard to accessing corporate Web sites and applications from your home or remote locations (typically involves use of VPN)?

Implementing Secure, Private, Reliable Computing

- Have you set the encryption method to WPA2 and changed the default name and password on your home wireless router?
- When using a free, public wireless network, do you avoid checking your email or accessing Web sites requiring a username and password?
- Do you refrain from clicking on a URL in an email from someone you do not know?
- Do you back up critical files to a separate device at least once a week?
- Are you familiar with and do you follow your organization's policies in regard to storing personal or confidential data on your device?

Implementing Secure, Private, Reliable Computing

- Does your device have a security passcode that must be entered before it accepts further input?
- Have you installed Locate My Device or similar software in case your device is lost or stolen?
- Do you make sure not to leave your device unattended in a public place where it can be easily stolen?

Implementing Secure, Private, Reliable Computing

Prevention

- No organization can ever be completely secure from attack.
- The key is to implement a layered security solution to make computer break-ins so difficult that an attacker eventually gives up.
- In a layered solution, if an attacker breaks through one layer of security, another layer must then be overcome.

Implementing Secure, Private, Reliable Computing

Detection

- Even when preventive measures are implemented, no organization is completely secure from a determined attack.
- Thus, organizations should implement detection systems to catch intruders in the act.
- Organizations often employ an intrusion detection system to minimize the impact of intruders.

Implementing Secure, Private, Reliable Computing

Response

- An organization should be prepared for the worst. A response plan should be developed well in advance of any incident and be approved by both the organization's legal department and senior management. A well-developed response plan helps keep an incident under technical control.
- In a security incident, the primary goal must be to regain control and limit damage, not to attempt to monitor or catch an intruder. Sometimes system administrators take the discovery of an intruder as a personal challenge and lose valuable time that should be used to restore data and information systems to normal.

Implementing Secure, Private, Reliable Computing

Computer Forensics

- *Computer forensics* is a discipline that combines elements of law and computer science to identify, collect, examine, and preserve data from computer systems, networks, and storage devices in a manner that preserves the integrity of the data gathered so that it is admissible as evidence in a court of law.
- A computer forensics investigation may be opened in response to a criminal investigation or civil litigation. It may also be launched for a variety of other reasons, for example, to retrace steps taken when data has been lost, assess damage following a computer incident, investigate the unauthorized disclosure of personal or corporate confidential data, or to confirm or evaluate the impact of industrial espionage.



Case Study: Change Healthcare Ransomware Attack (2024)

- **Overview:**

In February 2024, Change Healthcare, a major healthcare technology company responsible for processing insurance claims and pharmacy transactions, was hit by a massive ransomware attack. The attack disrupted critical healthcare services across the U.S., affecting hospitals, pharmacies, and insurance providers.

Case Study: Change Healthcare Ransomware Attack (2024)

Attack Details:

- **Threat Actor:** The ransomware group known as **ALPHV/BlackCat** claimed responsibility.
- **Method:** The attackers exploited vulnerabilities in remote access systems and deployed ransomware to encrypt data and disrupt operations.
- **Impact:**
 - Billing and payment systems were paralyzed for weeks.
 - Pharmacies couldn't process prescriptions, causing delays in patient care.
 - Sensitive patient data was exfiltrated, including medical records and insurance details.

Case Study: Change Healthcare Ransomware Attack (2024)

- **Financial Consequences:**
- Change Healthcare reportedly paid a **\$22 million ransom in Bitcoin** to regain access to its systems.
- The company faced losses exceeding **\$1 billion** due to operational downtime and recovery costs.

Case Study: Change Healthcare Ransomware Attack (2024)

- **Lessons Learned:**
- The incident highlighted the importance of:
 - **Multi-Factor Authentication (MFA)** for remote access.
 - Regular **patching and vulnerability management**.
 - Robust **incident response plans** and **data backup strategies**.

Summary

- Computer crime is a serious and rapidly growing area of concern requiring management attention.
- The number of cybercrimes being committed against individuals, organizations, and governments continues to increase, and the destructive impact of these crimes is also intensifying.
- The security of data and information systems used in business is of the utmost importance, but it must be balanced against other business needs.
- Increasing computing complexity, higher computer user expectations, expanding and changing systems, an increase in the prevalence of bring your own device (BYOD) policies, a growing reliance on software with known vulnerabilities, and the increasing sophistication of those who would do harm have caused a dramatic increase in the number, variety, and severity of security incidents.

Summary

- Many different types of people launch computer attacks, including the hacker, cracker, malicious insider, industrial spy, cybercriminal, hacktivist, and cyberterrorist. Each type has a different motivation.
- Ransomware, viruses, worms, Trojan horses, spam, distributed denial-of-service attacks, phishing, identity theft, and cyberespionage, are among the most common computer exploits.
- Organizations must take strong measures to ensure secure, private, and reliable computing experiences for their employees, customers, and business partners.
- A strong security program begins by assessing threats to the organization's computers and network, identifying actions that address the most serious vulnerabilities, and educating users about the risks involved and the actions they must take to prevent a security incident.

Summary

- The IS security group must lead the effort to implement security policies and procedures, as well as effectively employing available hardware and software tools to help prevent security breaches.
- Risk assessment is the process of assessing security related risks to an organization's computers and networks from both internal and external threats.
- No organization can ever be completely secure from attack. The key to prevention of a computer security incident is to implement a layered security solution to make computer break ins so difficult that an attacker eventually gives up.

Summary

- No security system is perfect, so systems and procedures must be monitored to detect a possible intrusion.
- If an intrusion occurs, there must be a clear reaction plan that addresses notification, evidence protection, activity log maintenance, containment, eradication, and follow-up.
- Organizations must be knowledgeable of and have access to trained experts in computer forensics to identify, collect, examine, and preserve data from computer systems, networks, and storage devices in a manner that preserves the integrity of the data gathered so that it is admissible as evidence in a court of law.

Reference

