សាកលវិទ្យាល័យភូមិន្ទភ្នំពេញ

ROYAL UNIVERSITY OF PHNOM PENH

Cybercrime and Information System Security

MIS

Chea Daly

Did You Know?

- Cybercrime is a serious and rapidly growing area of concern requiring management attention.
- The security of data and information systems used in business is of utmost importance.

Why Learn about Cybercrime and Information System Security?

- Although the need for security is obvious, it must often be balanced against other business needs.
- There is a number of trade-offs regarding IS security, such as:
  - How much effort and money should be spent to safeguard against computer crime? (In other words, how safe is safe enough?)

Why Learn about Cybercrime and Information System Security?

- If a firm is a victim of a computer crime, should it pursue prosecution of the criminals at all costs, maintain a low profile to avoid the negative publicity, inform affected customers, or take some other action?

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 Threat Landscape

- 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.

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 millions personal computers and mobile devices, all capable of sharing information, connect to networks.

Why Computer Incidents Are So Prevalent

- Businesses have moved quickly into e-commerce, collaborative work groups, global business, and interorganizational information systems.

Why Computer Incidents Are So Prevalent

- Increased Prevalence of Bring Your Own Device Policies
  - Most companies have found they cannot entirely prevent employees from using their own devices to perform work functions.
  - This raises many potential security issues as such devices are also used for nonwork activity (browsing Web sites, shopping, visiting social networks, etc.) that exposes them to malware frequently. That malware may then be spread throughout the company.

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.

TABLE 13.1 Total number of new software vulnerabilities identified annually

Year	Number of Software Vulnerabilities Identified
2007	7,540
2008	8,369
2009	7,716
2010	9,747
2011	9,307
2012	9,875
2013	13,075
2014	15,435

Why Computer Incidents Are So Prevalent

- While one would hope that the discoverer of a zero-day vulnerability (a newly discovered software vulnerability) would immediately inform the original software manufacturer so that a fix can be created for the problem.

Why Computer Incidents Are So Prevalent

- In some cases, this knowledge is sold on the black market to cyberterrorists, governments, or large organizations that may then use it to launch their own cyberattacks.
- For example, information about one zero-day vulnerability in Apple's iOS reportedly sold for $500,000.

Why Computer Incidents Are So Prevalent

- U.S. government keep information about vulnerabilities secret in cases in which government security experts have determined that the hole has “a clear national security or law enforcement” use.
- Packages of zero-day exploits have been sold to U.S. government for $2.5 million a year.

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.

Why Computer Incidents Are So Prevalent

- Today's computer menace is much better organized and may be part of an organized groups that have ample resources, including money and sophisticated tools to support their efforts.

TABLE 13.2 Classifying perpetrators of computer crime

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

Types of Exploits

There are numerous types of computer attacks, with new varieties being invented all the time. Such as:

- Ransomware
- Viruses
- Worms
- Trojan Horses
- Phishing
- …

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.
- 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.

Ransomware

- Ransomware can also be spread through removable USB drives or Yahoo Messenger, with the payload disguised as an image.

Ransomware Case: Hollywood Presbyterian Medical Center

- Hollywood Presbyterian Medical Center was forced to shut down its computer network after hackers encrypted some of its data in February, 2016.
- Initially, the hospital refused to pay the ransom, and hospital employees were forced to resort to paper, pencil, phones, and fax machines to carry out many of their tasks.

Ransomware Case: Hollywood Presbyterian Medical Center

- The hospital sought help from the FBI, the Los Angeles Police Department, and cybersecurity consultants, but it was never able to access to the data.
- After a week, the hospital paid the ransom of $12,000. By February 15, access to the data was fully restored and there was no evidence that any patient or employee data had been accessed.

Viruses

- Computer Virus is a piece of programming code, usually disguised as something else, that causes a computer to behave in an 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.

Viruses

- 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.

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.
- 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.

Worms

- The cost to repair the damage done by each of the Code Red, SirCam, and Melissa worms was estimated to exceed $1 billion, with that of the Conficker, Storm, and ILOVEYOU worms was totaling well over $5 billion.

Trojan Horses

- A Trojan horse is a 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 use.

Trojan Horses

- A Trojan horse can be delivered via an email attachment, downloaded to a user's computers when he or she visits a Web site, or contracted via a removable device.
- Common host programs include screen savers and games.

Trojan Horses

- Once a user executes the program that hosts the Trojan horse, the malicious payload is automatically launched as well—with no telltale signs.
- It might be designed to enable the hacker to destroy hard drives, 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.

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.

Phishing

- 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.

Phishing

- The volume of global phishing attacks is alarming. It is estimated that about 156 million phishing emails are sent each day, with 16 million of those successfully evading email filters. Of those, roughly 50 percent (or 8 million) are opened, and 800,000 recipients per day click on malicious URL links contained in the emails.

Data Breach

- A data breach is the unintended release of sensitive data or the access of sensitive data by unauthorized individuals, often resulting in identify theft.

Data Breach

TABLE 13.3 Five largest data breaches in the United States

Organization	Year	Number of Records Compromised	Data Stolen
Heartland Payment Systems	2008	130 million	Credit and debit card data
Target	2013	110 million	Credit and debit card data
Sony Online Entertainment Systems	2011	102 million	Login credentials, names, addresses, phone numbers, email addresses
Anthem	2015	80 million	Names, addresses, dates of birth, Social Security numbers, health insurance ID numbers
National Archives and Records Administration	2008	76 million	Names and contact information, Social Security numbers

Data Breach Case: Ashley Madison

- Some 37 million customer records of Ashley Madison (a Web site for married people seeking other married people with whom to have affairs) were attacked in 2015.
- Names and addresses were posted publicly, resulting in several lawsuits against the company for failing to safeguard the personal information.
- The security system was improved since the 2015 data breach, no accidents since then.

Federal Laws for Prosecuting Computer Attacks

- Over the years, several laws have been enacted to help prosecute those responsible for computer-related crime.
- For example, Identity Theft and Assumption Deterrence Act (U.S. Code Title 18, Section 1028) makes identity theft a federal crime, with penalties of up to 15 years' of imprisonment and a maximum fine of $250,000

Implementing Secure, Private, Reliable Computing

- Organizations worldwide are increasingly demanding methods of computing that deliver secure, private, and reliable computing experiences.
- Software and hardware manufacturers, consultants, and system designers and developers all understand that this is a priority for their customers.

Implementing Secure, Private, Reliable Computing

- 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 to ensure an effective response and recovery.

Implementing Secure, Private, Reliable Computing

- Risk Assessment
- Establishing a Security Policy
- Educating Employees
- Prevention
- Detection
- Response

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.
- 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.

Establishing a Security Policy

- A security policy outlines what needs to be done but not how to do it.
- Such as email policy, password protection policy, remote access policy, and so on.
- For example, a written policy states that passwords must be changed every 30 days.

Educating Employees

- Employees must be educated about the importance of security so that they will be motivated to understand and follow security policies.
- Users must understand that they are a key part of the security system and that they have certain responsibilities.

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.

Prevention

These layers of protective measures are:

- Implementing a Corporate Firewall
- Installing Antivirus Software on Personal Computers
- Implementing Safeguards against Attacks by Malicious Insiders
- Addressing the Most Critical Internet Security Threats
- Conducting Periodic IT Security Audits

Implementing a Corporate Firewall

- A firewall is a system of software, hardware, or a combination of both that stands guard between an organization's internal network and the Internet and limits network access based on the organization's access policy.
- Any Internet traffic that is not explicitly permitted into the internal network is denied entry through a firewall.

Implementing a Corporate Firewall

- Similarly, most firewalls can be configured so that internal network users can be blocked from gaining access to certain Web sites based on some content.
- Most firewalls can also be configured to block instant messaging, access to newsgroups, and other Internet activities.

Implementing a Corporate Firewall

- Software vendors Agnitum, Check Point, Comodo, Kaspersky, and Total Defense provide some of the top-rated firewall software used to protect personal computers.
- Their software provide antivirus, firewall, antispam, parental control, and phishing protection capabilities and sell for $30 to $80 per single user license.

Installing Antivirus Software on Personal Computers

- Antivirus software should be installed on each user's personal computer to scan a computer's memory and disk drives regularly for viruses.
- It is crucial that antivirus software be continually updated.
- Unfortunately, antivirus software is not able to identify and block all viruses.

Implementing Safeguards against Attacks by Malicious Insiders

- User accounts that remain active after employees leave a company are another potential security risk.
- To reduce the threat of attack by malicious insiders, IS staff must promptly delete the computer.

Implementing Safeguards against Attacks by Malicious Insiders

- Another important safeguard is to create roles and user accounts so that users have the authority to perform their responsibilities and nothing more.
- For example, members of the Finance Department should have different authorizations from members of the Human Resources Department.

Addressing the Most Critical Internet Security Threats

- The majority of successful computer attacks take advantage of well-known vulnerabilities.
- Computer attackers know that many organizations are slow to fix problems, which makes scanning the Internet for vulnerable systems an effective attack strategy.

Addressing the Most Critical Internet Security Threats

- It is good to keeping software and operating systems up-to-date.
- Those responsible for computer security must make it a priority to prevent attacks using these vulnerabilities.

Conducting Periodic IT Security Audits

- Another important prevention tool is a security audit that evaluates whether an organization has a well security policy and if it is being followed.
- For example, if a policy says that all users must change their passwords every 30 days, the audit must check how well that policy is being implemented.

Conducting Periodic IT Security Audits

- The audit should also review who has access to particular systems and data and what level of authority each user has.
- Tests might include trying the default system passwords that are active when software is first received from the vendor to ensure that all such known passwords have been changed.

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.

Detection

- An **intrusion detection system** (IDS) is software and/or hardware that monitors system and network resources and activities and notifies network security personnel when it detects network traffic that attempts to circumvent the security measures of a networked computer environment

Detection

- Two fundamentally different approaches to intrusion detection:
  - Knowledge-based approaches
  - behavior-based approaches

Detection

- Knowledge-based intrusion detection systems contain information about specific attacks and system vulnerabilities and watch for attempts to exploit these vulnerabilities.
  - such as repeated failed login attempts or recurring attempts to download a program to a server.
- When such an attempt is detected, an alarm is triggered.

Detection

- A behavior-based intrusion detection system compares current activity to the normal behaviors of the system and the users, and generates an alarm if it finds a deviation.
  - Examples include unusual traffic at odd hours or a user in the HR Department who accesses an accounting program that she has never before used.

Response

- An organization should be prepared for the worst—a successful attack that defeats all or some of a system's defenses and damages data and information systems.
- An incident response plan should be developed well in advance of any incident.
- A well-developed incident response plan helps keep an incident under technical and emotional control.

Response

- 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.

Response

- Incident Notification
  - A key element of any response plan is to define who to notify in the event of a computer security incident.
  - A critical ethical decision that must be made is what to tell customers and others whose personal data may have been compromised by a computer incident.

Response

- Many organizations are tempted to conceal such information for fear of bad publicity and loss of customers.
- Because such inaction is perceived by many to be unethical and harmful, a number of state and federal laws have been passed to force organizations to reveal when customer data has been breached.

Response

- Protection of Evidence and Activity Logs
  - An organization should document all details of a security incident.
  - It is especially important to capture all system events, the specific actions taken (what, when, and who) in a logbook.

Response

- Incident Containment
  - Often, it is necessary to act quickly to contain an attack and to keep a bad situation from becoming even worse.
  - The incident response plan should clearly define the process for deciding if an attack is dangerous enough to warrant shutting down or disconnecting critical systems from the network.

Response

- How such decisions are made, how fast they are made, and who makes them are all elements of an effective response plan.

Response

- Eradication
  - After the threat has been contained, it is necessary to eradicate (remove) malicious content. Make sure that this is done without losing precious data.
  - After virus eradication, a new backup must be created.

Response

- Incident Follow-Up
  - Write a formal incident report that includes a detailed chronology of events and the impact of the incident.
  - This report should identify any mistakes so that they are not repeated in the future.

Response

- The experience from this incident should be used to update and revise the security incident response plan.
- Creating a detailed chronology of all events will also document the incident for possible later prosecution.
- Another important issue is the amount of effort that should be put into capturing the perpetrator.

Cyber Crime Statistics (Updated February 2023)

- Through the pandemic, cyber criminals took advantage of misaligned networks as businesses moved to remote work environments. In 2020, malware attacks increased 358% compared to 2019.
- In 2021, nearly 1 billion emails exposed, affecting 1 in 5 internet users.

https://aag-it.com/the-latest-cyber-crime-statistics/

Cyber Crime Statistics (Updated February 2023)

- It is clear that the rate and cost of data breaches are increasing. Since 2001, the victim count has increased from 6 victims per hour to 97.
- Around 236.1 million ransomware attacks were reported worldwide in the first half of 2022.

Cyber Crime Statistics (Updated February 2023)

- The UK had the highest number of cyber crime victims per million internet users at 4783 in 2022.
- The country with the next highest number of victims per million internet users in 2022 was the USA, with 1494, a 13% decrease over 2020.
- 1 in 2 North American internet users had their accounts breached in 2021.

Cyber Crime Statistics (Updated February 2023)

- Between Q2 and Q3 of 2022, the countries that have suffered the largest increases in data breaches are:
  - China (4852% amounting to 14,157,775 breached accounts)
  - Japan (1423% amounting to 1,246,373 breached accounts)
  - South Korea (1007% amounting to 1,669,124 breached accounts)

Cyber Crime Statistics (Updated February 2023)

- In 2021, Asian organizations suffered the most attacks worldwide. The percentage of attacks against organizations by continent in 2021 is as follows:
  - Asia (26%)
  - Europe (24%)
  - North America (23%)
  - Middle East and Africa (14%)
  - Latin America (13%)

Cyber Crime Statistics (Updated February 2023)

- Facebook uncovered more than 400 malicious iOS and Android apps in 2022 that targeted mobile users to steal their Facebook login credentials.
  - 43% of these apps were ‘photo editors’, including ones that allowed the user to turn themselves into a cartoon.

Cyber Crime Statistics (Updated February 2023)

- A further 15% were ‘business utility’ apps, which claimed to be able to provide hidden features not found in official apps from reputable platforms.
- By creating fake reviews, cyber criminals can artificially inflate the ranking of their apps and disguise poor reviews that highlight issues.

Cyber Crime Statistics (Updated February 2023)

- Unsuspecting users then download the app, where they are then asked to log in using Facebook. Any details entered can be seen by the hacker.

Cyber Crime Statistics (Updated February 2023)

- Cyber criminals will use social media to scope out and target individuals for scams, such as romance scams.
  - This type of fraud involves the criminal establishing a ‘relationship’ with a target, before getting the unfortunate victim to send money, purportedly for plane tickets, an urgent operation or other ruses.

References

- **Reynolds, George Walter, Stair, Ralph M.** "Principles of information systems", 13e – 2018