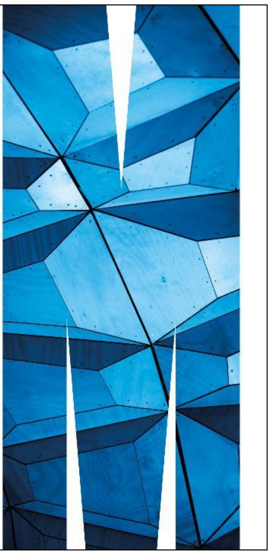
MONASH University

FIT2090
BUSINESS INFORMATION SYSTEMS AND PROCESSES

Lecture 11a IS in Society – Computer Crime

DRCLAYTON, FACULTY OF INFORMATION TECHNOLOGY
MONASH UNIVERSITY

GROUP OF EIGHT AUSTRALIA



Learning Objectives

On completion of this lecture, you will be able to:

- Identify and briefly describe the types of computer exploits and their impact
- Identify specific measures used to prevent computer crime

Why Computer Incidents Are So Prevalent ?

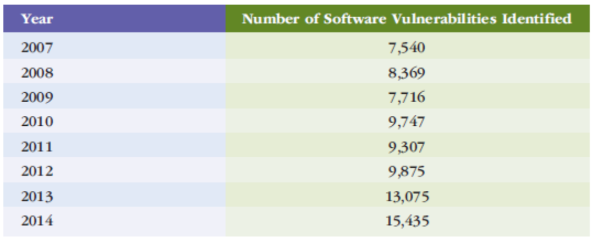
- Increasing Complexity Increases Vulnerability
  - Cloud computing, networks, computers, mobile devices, virtualization, OS applications, Web sites, switches, routers, and gateways are interconnected and driven by millions of lines of code
- Higher Computer User Expectations
  - Computer help desks are under intense pressure to respond very quickly to users' questions
- Expanding and Changing Systems Introduce New Risks
  - It is 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): a business policy that permits (encourages) employees to use their own mobile devices to access company computing resources and applications
  - BYOD makes it difficult for IT organizations to adequately safeguard additional portable devices with various OSs and applications
- Growing Reliance on Commercial Software with Known Vulnerabilities
  - 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
  - Users should download and install patches for known fixes to software vulnerabilities
    - Any delay in doing so exposes the user to a potential security breach

Why Computer Incidents Are So Prevalent ?

TABLE 13.1 Total number of new software vulnerabilities identified annually



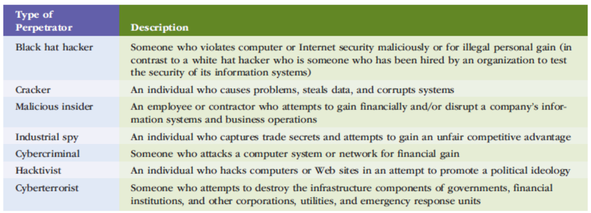
Year	Number of Software Vulnerabilities Identified
2007	7,540
2008	8,369
2009	7,716
2010	9,747
2011	9,307
2012	9,875
2013	13,075
2014	15,435

Pg 564, Stair and Reynold, 13th Ed

Why Computer Incidents Are So Prevalent ?

- Increasing Sophistication of Those Who Would Do Harm
  - Today's computer menace is organized and may be part of an organized group that has an agenda and targets specific organizations and Web sites

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

Pg 565, Stair and Reynold, 13th Ed

Types of Exploits

- Common attacks include:
  - Ransomware
  - Viruses
  - Worms
  - Trojan horses
  - Blended threat
  - Spam
  - Distributed denial-of-service attacks
  - Rootkits
  - Advanced persistent threat
  - Phishing, spear-phishing, smishing and vishing
  - Identity theft
  - Cyberespionage and cyberterrorism

Types of Exploits

- Ransomware
  - Malware that stops you from using your computer or accessing your data until you meet certain demands such as paying a ransom or sending photos to the attacker
- Viruses
  - A piece of programming code (usually disguised as something else) that causes a computer to behave in an unexpected and undesirable manner
  - Spread to other machines when a computer user shares an infected file or sends an email with a virus-infected attachment
- Worms
  - A harmful program that resides in the active memory of the computer and duplicates itself
  - Can propagate without human intervention

Types of Exploits

- Trojan Horses
  - A seemingly harmless program in which malicious code is hidden
  - A victim on the receiving end is usually tricked into opening it because it appears to be useful software from a legitimate source
    - The program's harmful payload might be designed to enable the attacker to destroy hard drives, corrupt files, control the computer remotely, launch attacks against other computers, steal passwords or spy on users
  - Often creates a "backdoor" on a computer that enables an attacker to gain future access
  - Logic bomb
    - A type of Trojan horse that executes when it is triggered by a specific event

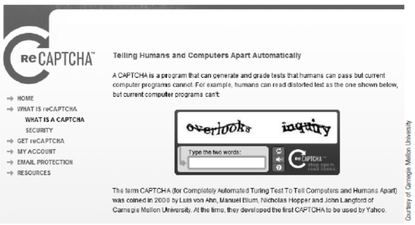
Types of Exploits

- Blended Threat
  - A sophisticated threat that combines the features of a virus, worm, Trojan horse, and other malicious code into a single payload
  - Might use server and Internet vulnerabilities to initiate and then transmit and spread an attack using EXE files, HTML files, and registry keys
- Spam
  - The use of email systems to send unsolicited email to large numbers of people
  - Also an inexpensive method of marketing used by many legitimate organizations
  - Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act states that it is legal to spam, provided the messages meet a few basic requirements
    - Spammers cannot disguise their identity by using a false return address
    - The email must include a label specifying that it is an ad or a solicitation
    - The email must include a way for recipients to opt out of future mass mailings

Types of Exploits

- Spam (cont'd)
  - 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

FIGURE 13.1
Example of CAPTCHA
CAPTCHA is used to distinguish humans from automated bots.



Telling Humans and Computers Apart Automatically

A CAPTCHA is a program that can generate and grade tests that humans can pass but current computer programs cannot. For example, humans can read distorted text as the one shown below, but current computer programs can't:

Type the two words:

The term CAPTCHA (for Completely Automated Turing Test To Tell Computers and Humans Apart) was coined in 2000 by Luis von Ahn, Manuel Blum, Nicholas Hopper and John Langford of Carnegie Mellon University. At the time, they developed the first CAPTCHA to be used by Yahoo.

Types of Exploits

- Distributed Denial-of-Service Attacks
  - An attack 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
  - Keeps target so busy responding to requests that legitimate users cannot get in
  - Botnet
    - A large group of computers, controlled from one or more remote locations by hackers, without the consent of their owners
    - Sometimes called zombies
    - Frequently used to distribute spam and malicious code

Types of Exploits

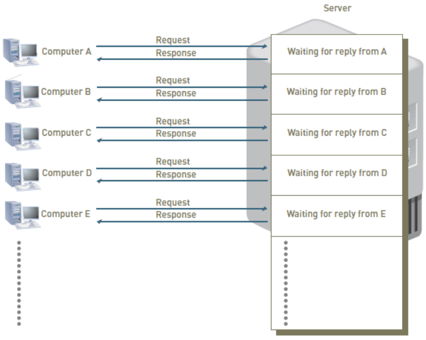


FIGURE 13.2
Distributed denial-of-service attack
A DDoS attack floods a target site with demands for data and other small tasks.

Types of Exploits

- Rootkit
  - A set of programs that enables its user to gain administrator-level access to a computer without the end user's consent or knowledge
  - Attackers can use the rootkit to execute files, access logs, monitor user activity, and change the computer's configuration
  - Symptoms of rootkit infections:
    - Computer locks up or fails to respond to input from the keyboard
    - Screen saver changes without any action on the part of the user
    - Taskbar disappears
    - Network activities function extremely slow

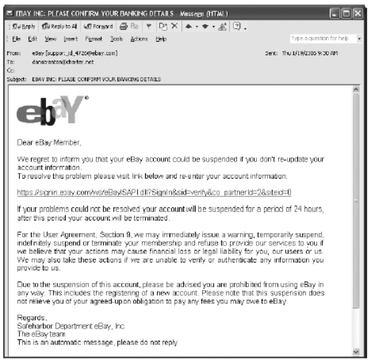
Types of Exploits

- Advanced Persistent Threat
  - APT is a network attack in which an intruder gains access to a network and stays undetected with the intention of stealing data over a long period of time
  - An APT attack advances through the following five phases:
    - Reconnaissance
    - Incursion
    - Discovery
    - Capture
    - Export
  - Detecting anomalies in outbound data is the best way for administrators to discover that the network has been the target of an APT attack

Types of Exploits

- Phishing
  - The act of fraudulently using email to try to get the recipient to reveal personal data
  - Con artists send legitimate-looking emails urging recipients to take action to avoid a negative consequence or to receive a reward
  - Spear-phishing is a variation of phishing where fraudulent emails are sent to a certain organization's employees
    - Much more precise and narrow
    - Designed to look like they came from high-level executives within organization

Types of Exploits



From: eBay [suppor_id_4720@ebay.com]
Sent: Thu 1/19/2006 9:30 AM
To: danscranton@charter.net
Cc:
Subject: EBAY INC: PLEASE CONFIRM YOUR BANKING DETAILS

Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

FIGURE 13.3
Example of phishing email
Phishing attacks attempt to get the recipient to reveal personal data.

Types of Exploits

- Smishing and Vishing
  - Smishing is a variation of phishing that involves the use of texting
  - Vishing is similar to smishing except the victims receive a voice mail message telling them to call a phone number or access a Web site
- Identity Theft
  - The theft of personal information and then used without their permission
  - Data breach is the unintended release of sensitive data or the access of sensitive data by unauthorized individuals
    - Often results in identity theft
  - Most e-commerce Web sites use some form of encryption technology to protect information as it comes from the consumer

Types of Exploits

- Cyberespionage
  - Involves the development of malware that secretly steals data in the computer systems of organizations, such as government agencies, military contractors, political organizations, and manufacturing firms
  - Mostly targeted toward high-value data such as 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

Types of Exploits

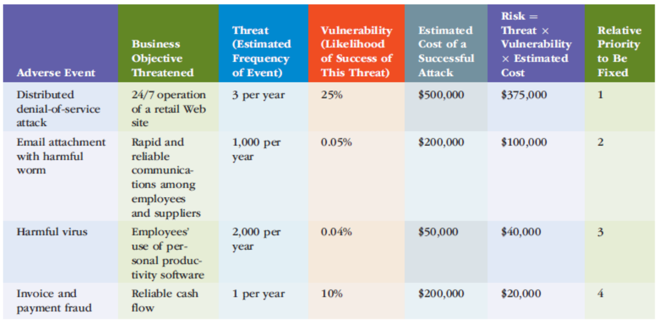
- Cyberterrorism
  - The intimidation of government of civilian population by using information technology to disable critical national infrastructure to achieve political, religious, or ideological goals
  - Department of Homeland Security (DHS) provides a link that enables users to report cyber incidents
    - Incident reports go to the U.S. Computer Emergency Readiness Team (US-CERT)
  - Cyberterrorists try daily to gain unauthorized access to a number of important and sensitive sites

Implementing Secure, Private, Reliable Computing

- A strong security program begins by
  - Assessing threats to the organization’s computers and network
  - Identifying actions that address the most serious vulnerabilities
  - Educating users about the risks involved and the actions they must take to prevent a security incident
- If an intrusion occurs, there must be a clear reaction plan that addresses:
  - Notification
  - Evidence protection
  - Activity log maintenance
  - Containment
  - Eradication
  - Recovery

Risk Assessment

TABLE 13.5 Risk assessment for a hypothetical company



Adverse Event	Business Objective Threatened	Threat (Estimated Frequency of Event)	Vulnerability (Likelihood of Success of This Threat)	Estimated Cost of a Successful Attack	Risk = Threat × Vulnerability × Estimated Cost	Relative Priority to Be Fixed
Distributed denial-of-service attack	24/7 operation of a retail Web site	3 per year	25%	$500,000	$375,000	1
Email attachment with harmful worm	Rapid and reliable communications among employees and suppliers	1,000 per year	0.05%	$200,000	$100,000	2
Harmful virus	Employees’ use of personal productivity software	2,000 per year	0.04%	$50,000	$40,000	3
Invoice and payment fraud	Reliable cash flow	1 per year	10%	$200,000	$20,000	4

Establishing a Security Policy

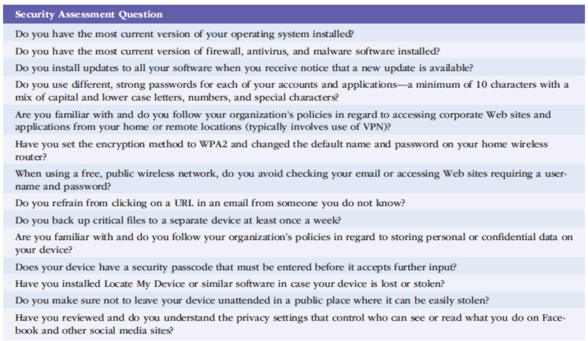
- Security policy
  - Defines an organization’s security requirements along with the controls and sanctions needed to meet those requirements
  - Outlines what needs to be done but not how to do it
- Automated system rules should mirror an organization’s written policies
- Some companies have begun to include special security requirements for mobile devices as part of their security policies

Educating Employees and Contract Workers

- Users can protect an organization’s information systems by:
  - 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
  - Taking care to ensure that portable computing and data storage devices are protected (hundreds of thousands of laptops are lost or stolen per year)

Educating Employees and Contract Workers

TABLE 13.6 Self-assessment security test



Security Assessment Question
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)?
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?
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?
Have you reviewed and do you understand the privacy settings that control who can see or read what you do on Facebook and other social media sites?

Prevention

- Organizations should implement a layered security solution to make computer break-ins so difficult that an attacker gives up
  - If an attacker breaks through one layer, another layer must then be overcome
- Layers of protective measures are explain in more detail in the following sections

Prevention

- Firewall
  - 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
- Next-generation firewall (NGFW)
  - A hardware- or software-based network security system that is able to detect and block sophisticated attacks by filtering network traffic dependent on the packet contents
  - Goes deeper to inspect the payload of packets and match sequences of bytes for harmful activities

Installing Antivirus Software on Personal Computers

- Antivirus software
  - Scans for specific sequence of bytes, known as a virus signature, that indicates the presence of a specific virus
- If virus is found
  - Antivirus software informs the user and may clean, delete, or quarantine any files, directories, or disks affected by the malicious code
- It is crucial that antivirus software be continually updated with the latest virus signatures

Implementing Safeguards against Attacks by Malicious Insiders

- User accounts that remain active after employees leave a company are a potential security risk
  - IS staff must promptly delete computer accounts, login IDs, and passwords of departing employees
- Another safeguard
  - Create roles and user accounts so that users have the authority to perform their responsibilities and nothing more

Conducting Periodic IT Security Audits

- Security audit
  - Evaluates whether an organization has well-considered security policy in place and if it is being followed
- The audit should
  - Review who has access to particular systems and data and what level of authority each user has
  - Test system safeguards to ensure that they are operating as intended
- Some organizations also perform a penetration test
  - Individuals try to break through the measures and identify vulnerabilities

Detection

- Intrusion detection system (IDS)
  - Software and/or hardware that monitors system and network resources and activities
  - Notifies network security personnel when it detects network traffic that attempts to circumvent the security measures of a networked computer environment
- Knowledge-based IDS
  - Contain information about specific attacks and system vulnerabilities
- Behaviour-based IDS
  - Models normal behaviour of a system and its user from reference information collected by various means

Detection

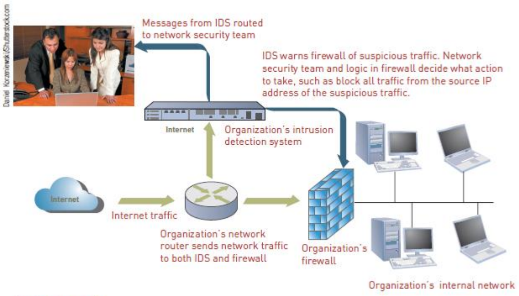

Daniel Korzeniewski/Shutterstock.com
Messages from IDS routed to network security team
IDS warns firewall of suspicious traffic. Network security team and logic in firewall decide what action to take, such as block all traffic from the source IP address of the suspicious traffic.
Internet
Organization's intrusion detection system
Internet
Internet traffic
Organization's network router sends network traffic to both IDS and firewall
Organization's firewall
Organization's internal network

FIGURE 13.5
Intrusion detection system
An IDS notifies network security personnel when it detects network traffic that attempts to circumvent the security measures of a networked computer environment.

Response

- A response plan should be developed well in advance of any incident
  - Should be approved by the organization's legal department and senior management
- A well-developed response plan helps keep an incident under technical and emotional 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

Protection of Evidence and Activity Logs

- Organizations should document all details of a security incident as it works to resolve the incident
- Documentation captures valuable evidence for a future prosecution
  - And provides data to help during the incident eradication and follow-up phases
- Organizations should establish a set of document-handling procedures using the legal department as a resource

Summary

- Computer crime is an international issue
- Security measures, e.g., using passwords, identification numbers, and data encryption, help to guard against illegal computer access
- Balancing the right to privacy versus the need for additional monitoring to protect against terrorism and cyberattacks is an especially challenging problem
- Employers use technology and corporate policies to manage worker productivity and protect the use of IS resources
- A business should develop a clear and thorough privacy policy