



Prifysgol Cymru  
Y Drindod Dewi Sant  
**University of Wales**  
Trinity Saint David

# ACCA5034

## Data Security and Compliance Week 2 :The need for Security

*Trawsnewid Addysg; Trawsnewid Bywydau*  
*Transforming Education; Transforming Lives*



[www.uwtsd.ac.uk](http://www.uwtsd.ac.uk)

# Learning Objective(s) and Key Concepts

## Learning Objective(s)

- Explain why we need Information Security
- Explore the different type of threats

## Key Concepts

- Define The need for Information Security
- Define the functions of an Information System security environment
- Explain how threats are evolving
- Understand the various threats



# Introduction to the Need for Information Security

- The primary mission of an information security program is to ensure that **information assets**—information and the systems that house them—remain safe and useful.
- If threats didn't exist, resources could be used exclusively to improve systems that contain, use, and transmit information.
- The threat of attacks on information systems is a constant concern.
- Organisations must understand the environment in which information assets reside so their information security programs can address actual and potential problems.



# Information Security Functions

- Information security performs four important functions for an organisation:
  - Protecting the organisation's ability to function
  - Protecting the data and information the organisation collects and uses
  - Enabling the safe operation of applications running on the organisation's IT systems
  - Safeguarding the organisation's technology assets

# Business Needs First

- When security needs and business needs collide, business wins.
- Without the underlying business to generate revenue and use the information, the information may lose value, and there would be no need for it.
- If the business cannot function, information security becomes less important.
- The key is to balance the needs of the organisation with the need to protect information assets, realizing that business needs come first.



# Protecting Functionality

- All three communities of interest are responsible for facilitating security programs.
- Implementing information security has more to do with management than technology.
- Communities of interest should address information security in terms of business impact and cost of business interruption, rather than isolating security as a technical problem.



# Protecting Data That Organisations Collect and Use

- Without data, an organisation loses its record of transactions and the ability to deliver value to customers.
- Protecting data in transmission, in processing, and at rest (storage) is a critical aspect of information security.
- Securing databases encompasses managerial, technical, and physical controls.



# Enabling the Safe Operation of Applications

- Organisations needs environment that safeguard applications using IT systems.
- Management must continue to oversee infrastructure once in place—not relegate it to the IT department.

# Safeguarding Technology Assets in organisations

- Organisations must employ secure infrastructure hardware appropriate to the size and scope of the enterprise.
- Additional security services may be needed as the organisation grows.
- More robust solutions should replace security programs the organisation has outgrown.
- IT continues to add new capabilities and methods that allow organisations to solve business information management challenges.



# Information Security Threats and Attacks

- Threat: A potential risk to an asset's loss of value.
- Attack: An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it.
- Exploit: A technique used to compromise a system.
- Vulnerability: A potential weakness in an asset or its defensive control system(s).
- Management must be informed about the various threats to an organisation's people, applications, data, and information systems.
- Overall security is improving, but the number of potential hackers is growing.

# Rated Threats from Internal Sources

## Survey of Threats to Information Protection

| From Employees or Internal Stakeholders                                    | Not a Threat<br>1 | 2     | 3     | 4     | A Severe Threat<br>5 | Comp. Rank |
|----------------------------------------------------------------------------|-------------------|-------|-------|-------|----------------------|------------|
| Inability/unwillingness to follow established policy                       | 6.6%              | 17.2% | 33.6% | 26.2% | 16.4%                | 66%        |
| Disclosure due to insufficient training                                    | 8.1%              | 23.6% | 29.3% | 25.2% | 13.8%                | 63%        |
| Unauthorised access or escalation of privileges                            | 4.8%              | 24.0% | 31.2% | 31.2% | 8.8%                 | 63%        |
| Unauthorised information collection/data sniffing                          | 6.4%              | 26.4% | 40.0% | 17.6% | 9.6%                 | 60%        |
| Theft of on-site organisational information assets                         | 10.6%             | 32.5% | 34.1% | 12.2% | 10.6%                | 56%        |
| Theft of mobile/laptop/tablet and related/<br>connected information assets | 15.4%             | 29.3% | 28.5% | 17.9% | 8.9%                 | 55%        |

# Rated Threats from Internal Sources

## Survey of Threats to Information Protection

| From Employees or Internal Stakeholders                                      | Not a Threat<br>1 | 2     | 3     | 4     | A Severe Threat<br>5 | Comp. Rank |
|------------------------------------------------------------------------------|-------------------|-------|-------|-------|----------------------|------------|
| Intentional damage or destruction of information assets                      | 22.3%             | 43.0% | 18.2% | 13.2% | 3.3%                 | 46%        |
| Theft or misuse of organisationally leased, purchased, or developed software | 29.6%             | 33.6% | 21.6% | 10.4% | 4.8%                 | 45%        |
| Web site defacement                                                          | 43.4%             | 33.6% | 16.4% | 4.9%  | 1.6%                 | 38%        |
| Blackmail of information release or sales                                    | 43.5%             | 37.1% | 10.5% | 6.5%  | 2.4%                 | 37%        |

# Rated Threats from External Sources

## Survey of Threats to Information Protection

| From Outsiders or External Stakeholders                                | Not a Threat<br>1 | 2     | 3     | 4     | A Severe Threat<br>5 | Comp. Rank |
|------------------------------------------------------------------------|-------------------|-------|-------|-------|----------------------|------------|
| Unauthorised information collection/data sniffing                      | 6.4%              | 14.4% | 21.6% | 32.8% | 24.8%                | 71%        |
| Unauthorised access or escalation of privileges                        | 7.4%              | 14.0% | 26.4% | 31.4% | 20.7%                | 69%        |
| Web site defacement                                                    | 8.9%              | 23.6% | 22.8% | 26.8% | 17.9%                | 64%        |
| Intentional damage or destruction of information assets                | 14.0%             | 32.2% | 18.2% | 24.8% | 10.7%                | 57%        |
| Theft of mobile/laptop/tablet and related/connected information assets | 20.5%             | 25.4% | 26.2% | 15.6% | 12.3%                | 55%        |
| Theft of on-site organisational information assets                     | 21.1%             | 24.4% | 25.2% | 17.9% | 11.4%                | 55%        |

# Rated Threats from External Survey of Threats to Information Protection

| From Outsiders or External Stakeholders                                      | Not a Threat<br>1 | 2     | 3     | 4     | A Severe Threat<br>5 | Comp. Rank |
|------------------------------------------------------------------------------|-------------------|-------|-------|-------|----------------------|------------|
| Blackmail of information release or sales                                    | 31.1%             | 30.3% | 14.8% | 14.8% | 9.0%                 | 48%        |
| Disclosure due to insufficient training                                      | 34.5%             | 21.8% | 22.7% | 13.4% | 7.6%                 | 48%        |
| Inability/unwillingness to follow established policy                         | 33.6%             | 29.4% | 18.5% | 6.7%  | 11.8%                | 47%        |
| Theft or misuse of organisationally leased, purchased, or developed software | 31.7%             | 30.1% | 22.8% | 9.8%  | 5.7%                 | 46%        |

# Perceived Threats to Information Assets

## Survey of Threats to Information Protection

| General Threats to Information Assets                                                      | Not a Threat<br>1 | 2     | 3     | 4     | A Severe Threat<br>5 | Comp. Rank |
|--------------------------------------------------------------------------------------------|-------------------|-------|-------|-------|----------------------|------------|
| Electronic phishing/spoofing attacks                                                       | 0.8%              | 13.1% | 16.4% | 32.0% | 37.7%                | 79%        |
| Malware attacks                                                                            | 1.7%              | 12.4% | 27.3% | 36.4% | 22.3%                | 73%        |
| Unintentional employee/insider mistakes                                                    | 2.4%              | 17.1% | 26.8% | 35.8% | 17.9%                | 70%        |
| Loss of trust due to information loss                                                      | 4.1%              | 18.9% | 27.0% | 22.1% | 27.9%                | 70%        |
| Software failures or errors due to unknown vulnerabilities in externally acquired software | 5.6%              | 18.5% | 28.2% | 33.9% | 13.7%                | 66%        |
| Social engineering of employees/insiders based on social media information                 | 8.1%              | 14.6% | 32.5% | 34.1% | 10.6%                | 65%        |
| Social engineering of employees/insiders based on other published information              | 8.9%              | 19.5% | 24.4% | 32.5% | 14.6%                | 65%        |

# Perceived Threats to Information Assets

## Survey of Threats to Information Protection

| General Threats to Information Assets                                                    | Not a Threat<br>1 | 2     | 3     | 4     | A Severe Threat<br>5 | Comp. Rank |
|------------------------------------------------------------------------------------------|-------------------|-------|-------|-------|----------------------|------------|
| Software failures or errors due to poorly developed, internally created applications     | 7.2%              | 21.6% | 24.0% | 32.0% | 15.2%                | 65%        |
| SQL injections                                                                           | 7.6%              | 17.6% | 31.9% | 29.4% | 13.4%                | 65%        |
| Social engineering of employees/insiders based on organisation's Web sites               | 11.4%             | 19.5% | 23.6% | 31.7% | 13.8%                | 63%        |
| Denial of service (and distributed DoS) attacks                                          | 8.2%              | 23.0% | 27.9% | 32.8% | 8.2%                 | 62%        |
| Software failures or errors due to known vulnerabilities in externally acquired software | 8.9%              | 23.6% | 26.8% | 35.8% | 4.9%                 | 61%        |
| Outdated organisational software                                                         | 8.1%              | 28.2% | 26.6% | 26.6% | 10.5%                | 61%        |

# Perceived Threats to Information Assets

## Survey of Threats to Information Protection

| General Threats to Information Assets                                     | Not a Threat<br>1 | 2     | 3     | 4     | A Severe Threat<br>5 | Comp. Rank |
|---------------------------------------------------------------------------|-------------------|-------|-------|-------|----------------------|------------|
| Loss of trust due to representation as source of phishing/spoofing attack | 9.8%              | 23.8% | 30.3% | 23.0% | 13.1%                | 61%        |
| Loss of trust due to Web defacement                                       | 12.4%             | 30.6% | 31.4% | 19.8% | 5.8%                 | 55%        |
| Outdated organisational hardware                                          | 17.2%             | 34.4% | 32.8% | 12.3% | 3.3%                 | 50%        |
| Outdated organisation data format                                         | 18.7%             | 35.8% | 26.8% | 13.8% | 4.9%                 | 50%        |
| Inability/unwillingness to establish effective policy by management       | 30.4%             | 26.4% | 24.0% | 13.6% | 5.6%                 | 48%        |
| Hardware failures or errors due to aging equipment                        | 19.5%             | 39.8% | 24.4% | 14.6% | 1.6%                 | 48%        |

# Perceived Threats to Information Assets

## Survey of Threats to Information Protection

| General Threats to Information Assets                                                                   | Not a Threat<br>1 | 2     | 3     | 4    | A Severe Threat<br>5 | Comp.<br>Rank |
|---------------------------------------------------------------------------------------------------------|-------------------|-------|-------|------|----------------------|---------------|
| Hardware failures or errors due to defective equipment                                                  | 17.9%             | 48.0% | 24.4% | 8.1% | 1.6%                 | 46%           |
| Deviations in quality of service from other provider                                                    | 25.2%             | 38.7% | 25.2% | 7.6% | 3.4%                 | 45%           |
| Deviations in quality of service from data communications provider/ISP                                  | 26.4%             | 39.7% | 23.1% | 7.4% | 3.3%                 | 44%           |
| Deviations in quality of service from telecommunications provider/ISP (if different from data provider) | 29.9%             | 38.5% | 18.8% | 9.4% | 3.4%                 | 44%           |
| Loss due to other natural disaster                                                                      | 31.0%             | 37.9% | 23.3% | 6.9% | 0.9%                 | 42%           |

# Perceived Threats to Information Assets

## Survey of Threats to Information Protection

| General Threats to Information Assets                | Not a Threat<br>1 | 2     | 3     | 4    | A Severe Threat<br>5 | Comp. Rank |
|------------------------------------------------------|-------------------|-------|-------|------|----------------------|------------|
| Loss due to fire                                     | 26.2%             | 49.2% | 21.3% | 3.3% | 0.0%                 | 40%        |
| Deviations in quality of service from power provider | 36.1%             | 43.4% | 12.3% | 5.7% | 2.5%                 | 39%        |
| Loss due to flood                                    | 33.9%             | 43.8% | 19.8% | 1.7% | 0.8%                 | 38%        |
| Loss due to earthquake                               | 41.7%             | 35.8% | 15.0% | 6.7% | 0.8%                 | 38%        |

# Common Attack Pattern Enumeration and Classification (CAPEC)

- A tool that security professionals can use to understand attacks is the Common Attack Pattern Enumeration and Classification (CAPEC) Web site hosted by Mitre—a nonprofit research and development organisation sponsored by the U.S. government.
- This online repository can be searched for characteristics of a particular attack or simply browsed by professionals who want additional knowledge of how attacks occur procedurally.

# The 12 Categories of Threats

# The 12 Categories of Threats to Information Security

| Category of Threat                    | Attack Examples                                                 |
|---------------------------------------|-----------------------------------------------------------------|
| Compromises to intellectual property  | Piracy, copyright infringement                                  |
| Deviations in quality of service      | Internet service provider (ISP), power, or WAN service problems |
| Espionage or trespass                 | Unauthorised access and/or data collection                      |
| Forces of nature                      | Fire, floods, earthquakes, lightning                            |
| Human error or failure                | Accidents, employee mistakes                                    |
| Information extortion                 | Blackmail, information disclosure                               |
| Sabotage or vandalism                 | Destruction of systems or information                           |
| Software attacks                      | Viruses, worms, macros, denial of service                       |
| Technical hardware failures or errors | Equipment failure                                               |
| Technical software failures or errors | Bugs, code problems, unknown loopholes                          |
| Technological obsolescence            | Antiquated or outdated technologies                             |
| Theft                                 | Illegal confiscation of equipment or information                |



# Compromises to Intellectual Property

- Intellectual property (IP): creation, ownership, and control of original ideas as well as the representation of those ideas
- IP includes trade secrets, copyrights, trademarks, and patents.
- The most common IP breaches involve software piracy.
- Two watchdog organisations investigate software abuse:
  - Software and Information Industry Association (SIIA)
  - Business Software Alliance (BSA)
- According to the BSA, approximately 37 percent of software installed on personal computers globally are not properly licensed.



# Deviations in Quality of Service

- An information system depends on the successful operation of many interdependent support systems.
- Internet service, communications, and power irregularities dramatically affect the availability of information and systems.
- Services are usually arranged with a service level agreement (SLA).

# Average Cost of Downtime According to Fusion Connect

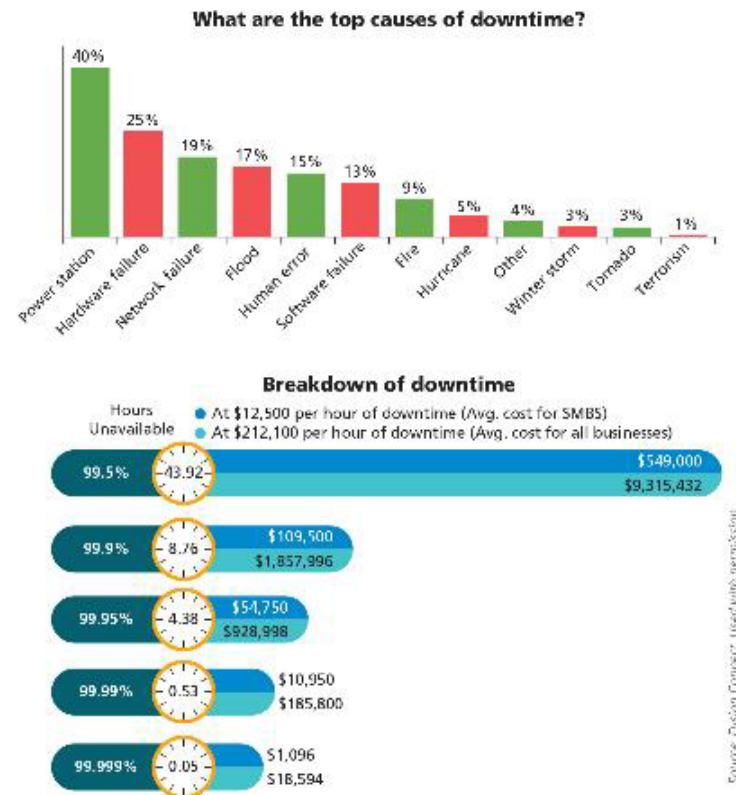


Figure 2-4 Average cost of downtime according to Fusion Connect<sup>12</sup>

# Deviations in Quality of Service (2 of 3)

- Internet service issues
  - Internet service provider (ISP) failures can considerably undermine the availability of information.
  - An outsourced Web hosting provider assumes responsibility for all Internet services as well as for the hardware and Web site operating system software.
- Communications and other service provider issues
  - Other utility services affect organisations: telephone, water, wastewater, trash pickup.



# Deviations in Quality of Service

- Power irregularities
  - Commonplace
  - Lead to fluctuations such as power excesses, power shortages, and power losses (blackout, brownout, fault, noise, sag, spike, or surge)
  - Sensitive electronic equipment vulnerable to and easily damaged/destroyed by fluctuations
  - Controls can be applied to manage power quality.

# Espionage or Trespass

## Shoulder Surfing



- Access of protected information by unauthorised individuals
- Competitive intelligence techniques are legal, whereas industrial espionage techniques are not.
- Shoulder surfing can occur anywhere a person accesses confidential information.
- Acts of trespass can lead to unauthorised real or virtual actions that enable information gatherers to enter premises or systems without permission.
- Hackers use skill, guile, or fraud to bypass controls protecting others' information.



# Espionage or Trespass

- Expert hacker
  - Develops software scripts and program exploits
  - Usually a master of many skills
  - Will often create attack software and share with others
- Unskilled hackers
  - Many more unskilled hackers than expert hackers
  - Use expertly written software to exploit a system
  - Do not usually fully understand the systems they hack
  - Also known as script kiddies or packet monkeys



# Espionage or Trespass

- Other terms for system rule breakers:
  - Cracker: “cracks” or removes software protection designed to prevent unauthorised duplication.
  - Phreaker: hacks the public telephone system to make free calls or disrupt services.
- Password attacks
  - Cracking
  - Brute force
  - Dictionary
  - Rainbow tables
  - Social engineering

# Password Strength

- Case-insensitive Passwords Using a Standard Alphabet Set (No Numbers or Special Characters)

| Password Length | Odds of Cracking               | Estimated Time to Crack* |
|-----------------|--------------------------------|--------------------------|
| 8               | 208,827,064,576                | 0.36 seconds             |
| 10              | 141,167,095,653,376            | 4.02 minutes             |
| 12              | 95,428,956,661,682,200         | 1.89 days                |
| 14              | 64,509,974,703,297,200,000     | 3.5 years                |
| 16              | 43,608,742,899,428,900,000,000 | 2,362.1 years            |

- Case-sensitive Passwords Using a Standard Alphabet Set (with Numbers and 20 Special Characters)

| Password Length | Odds of Cracking:                         | Estimated Time to Crack* |
|-----------------|-------------------------------------------|--------------------------|
| 8               | 2,044,140,858,654,980                     | 1.0 hours                |
| 10              | 13,744,803,133,596,100,000                | 271.7 days               |
| 12              | 92,420,056,270,299,900,000,000            | 5,006.0 years            |
| 14              | 621,432,458,361,496,000,000,000,000       | 33,660,438.6 years       |
| 16              | 4,178,511,850,022,700,000,000,000,000,000 | 226,332,789,392.1 years  |



# Forces of Nature

- Forces of nature can present some of the most dangerous threats.
- They disrupt not only individual lives, but also storage, transmission, and use of information.
- Threats include fires, floods, earthquakes, lightning, landslides, tornados, hurricanes, tsunamis, ESD, dust contamination, solar activity, civil unrest, and acts of war.
- Organisations must implement controls to limit damage and prepare contingency plans for continued operations.



# Human Error or Failure

- Includes acts performed without malicious intent or in ignorance
- Causes include:
  - Inexperience
  - Improper training
  - Incorrect assumptions
- Employees are among the greatest threats to an organisation's data.

# The Biggest Threat—Acts of Human Error or Failure

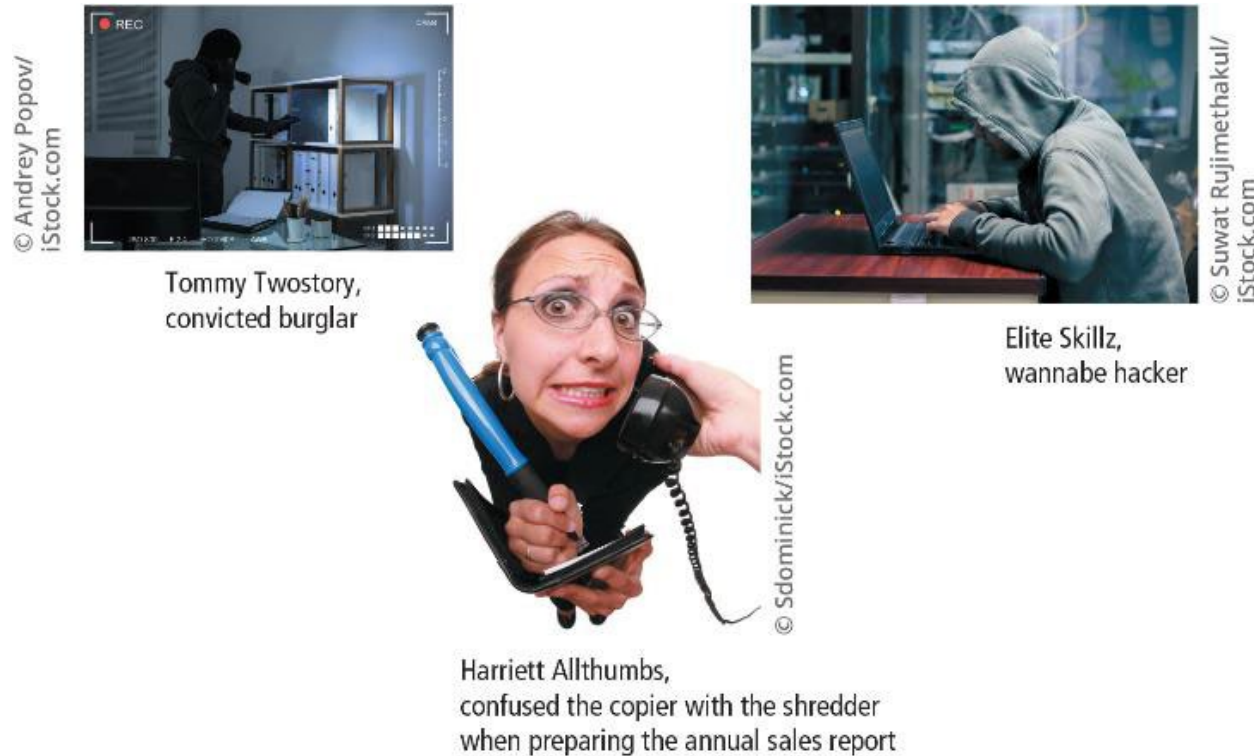


**Figure 2-8** The biggest threat—acts of human error or failure



# Human Error or Failure

- Employee mistakes can easily lead to:
  - Revelation of classified data
  - Entry of erroneous data
  - Accidental data deletion or modification
  - Data storage in unprotected areas
  - Failure to protect information
- Many of these threats can be prevented with training, ongoing awareness activities, and controls.
- Social engineering uses social skills to convince people to reveal access credentials or other valuable information to an attacker.



# Social Engineering

- Business e-mail compromise: exploiting business e-mail systems and users
- Advance-fee fraud: indicates recipient is due money and small advance fee or personal banking information required to facilitate transfer
- Phishing: attempt to gain personal/confidential information; apparent legitimate communication hides embedded code that redirects user to third-party site

# Phishing Example: Lure

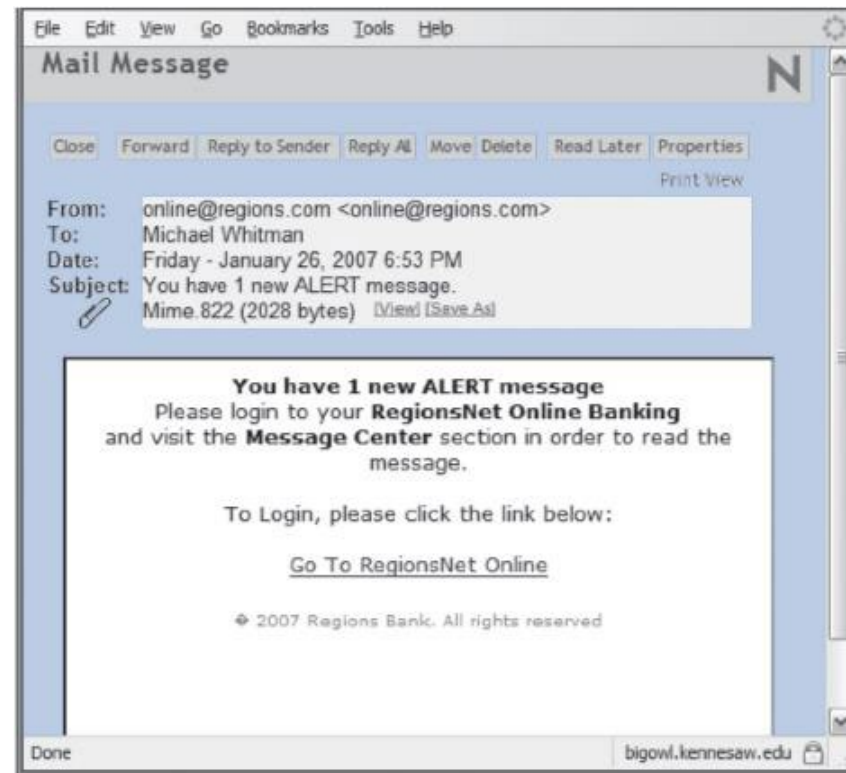


Figure 2-10 Phishing example: lure

# Phishing Example: Fake Website

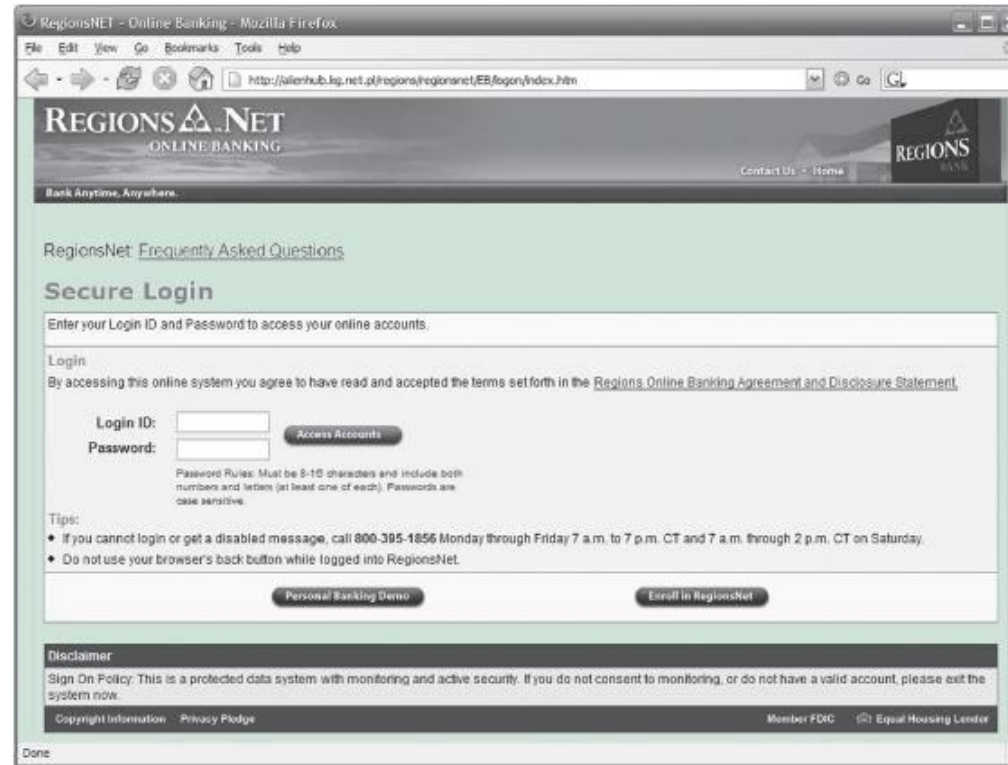


Figure 2-11 Phishing example: fake Web site



# Information Extortion

- Also known as cyberextortion
- Attacker steals information from a computer system and demands compensation for its return or nondisclosure
- Common in credit card number theft

# Ransomware

- Ransomware is a malware attack on the host system that denies access to the user and then offers to provide a key to allow access back to the user's system and data for a fee.
- There are two types of ransomware: lockscreen and encryption.
- Common phishing mechanisms to get a user to download ransomware include pop-ups indicating that illegal information or malware was detected on the user's system, threatening to notify law enforcement, or offering to delete the offending material if the user clicks a link or button.

# Ransomware Notification Screen



Figure 2-13 Ransomware notification screen



# Sabotage or Vandalism

- Threats can range from petty vandalism to organised sabotage.
- Web site defacing can erode consumer confidence, diminishing an organisation's sales, net worth, and reputation.
- Threat of hacktivist or cyberactivist operations is rising.
- Cyberterrorism/cyberwarfare: a much more sinister form of hacking



# Software Attacks

- Malicious software (malware) is used to overwhelm the processing capabilities of online systems or to gain access to protected systems via hidden means.
- Software attacks occur when an individual or a group designs and deploys software to attack a system.
- When an attack makes use of malware that is not yet known by the antimalware software companies, it is said to be a zero-day attack.



# Type of Software Attacks

- Malware (malicious code): It includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.
  - Virus: It consists of code segments that attach to existing program and take control of access to the targeted computer.
  - Worms: They replicate themselves until they completely fill available resources such as memory and hard drive space.
  - Trojan horses: malware disguised as helpful, interesting, or necessary pieces of software
  - Polymorphic threat: actually evolves to elude detection
  - Virus and worm hoaxes: nonexistent malware that employees waste time spreading awareness about
  - Back door: gaining access to system or network using known or previously unknown/newly discovered access mechanism



# Type of Software Attacks

- Types of attacks (cont'd)
  - Denial-of-service (DoS): An attacker sends a large number of connection or information requests to a target.
    - The target system becomes overloaded and cannot respond to legitimate requests for service.
    - It may result in a system crash or inability to perform ordinary functions.
  - Distributed denial-of-service (DDoS): A coordinated stream of requests is launched against a target from many locations simultaneously.

# Denial-of-Service Attacks

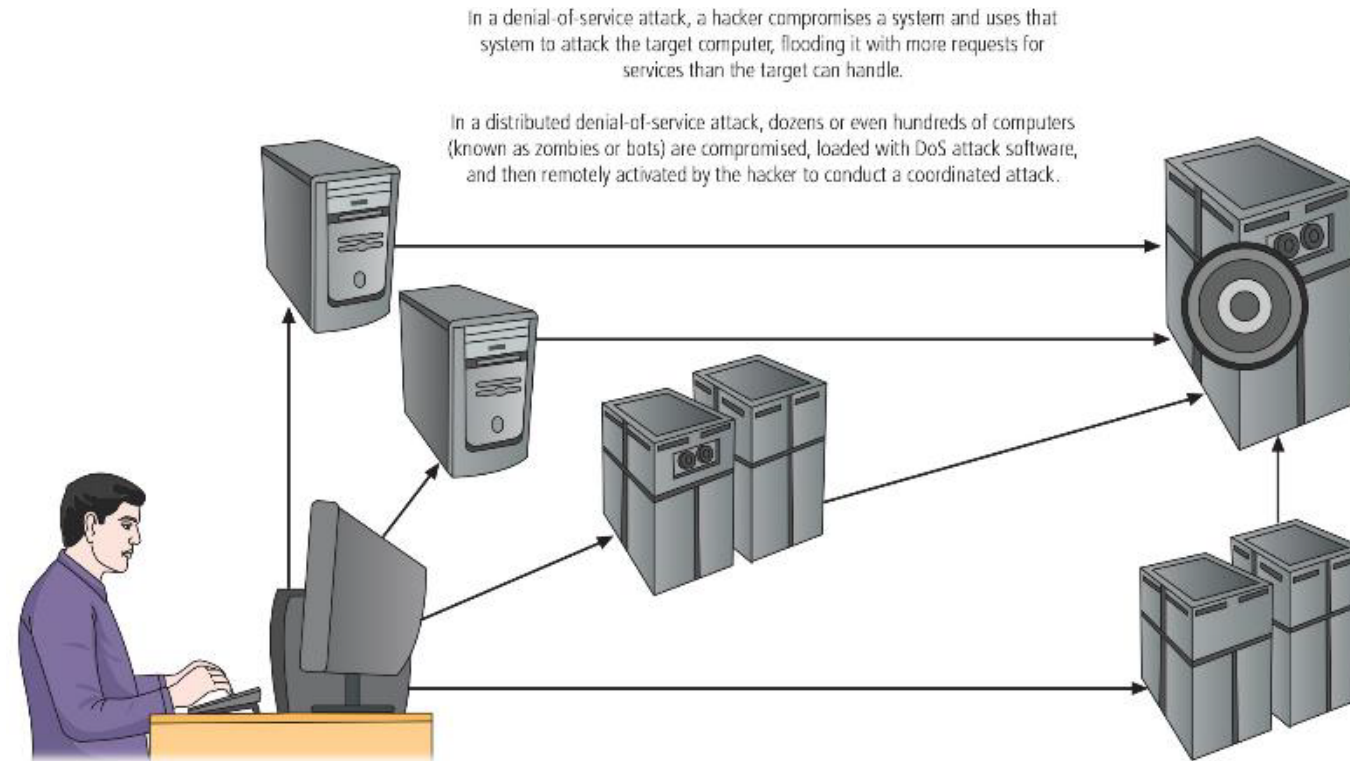


Figure 2-16 Denial-of-service attacks



# Type of Software Attacks

- Types of attacks (cont'd)
  - Mail bombing (also a DoS): An attacker routes large quantities of e-mail to a target to overwhelm the receiver.
  - Spam (unsolicited commercial e-mail): It is considered more a nuisance than an attack, though it is emerging as a vector for some attacks.
  - Packet sniffer: It monitors data traveling over a network; it can be used both for legitimate management purposes and for stealing information from a network.
  - Spoofing: A technique used to gain unauthorised access; an intruder assumes a trusted IP address.

# IP Spoofing Attack

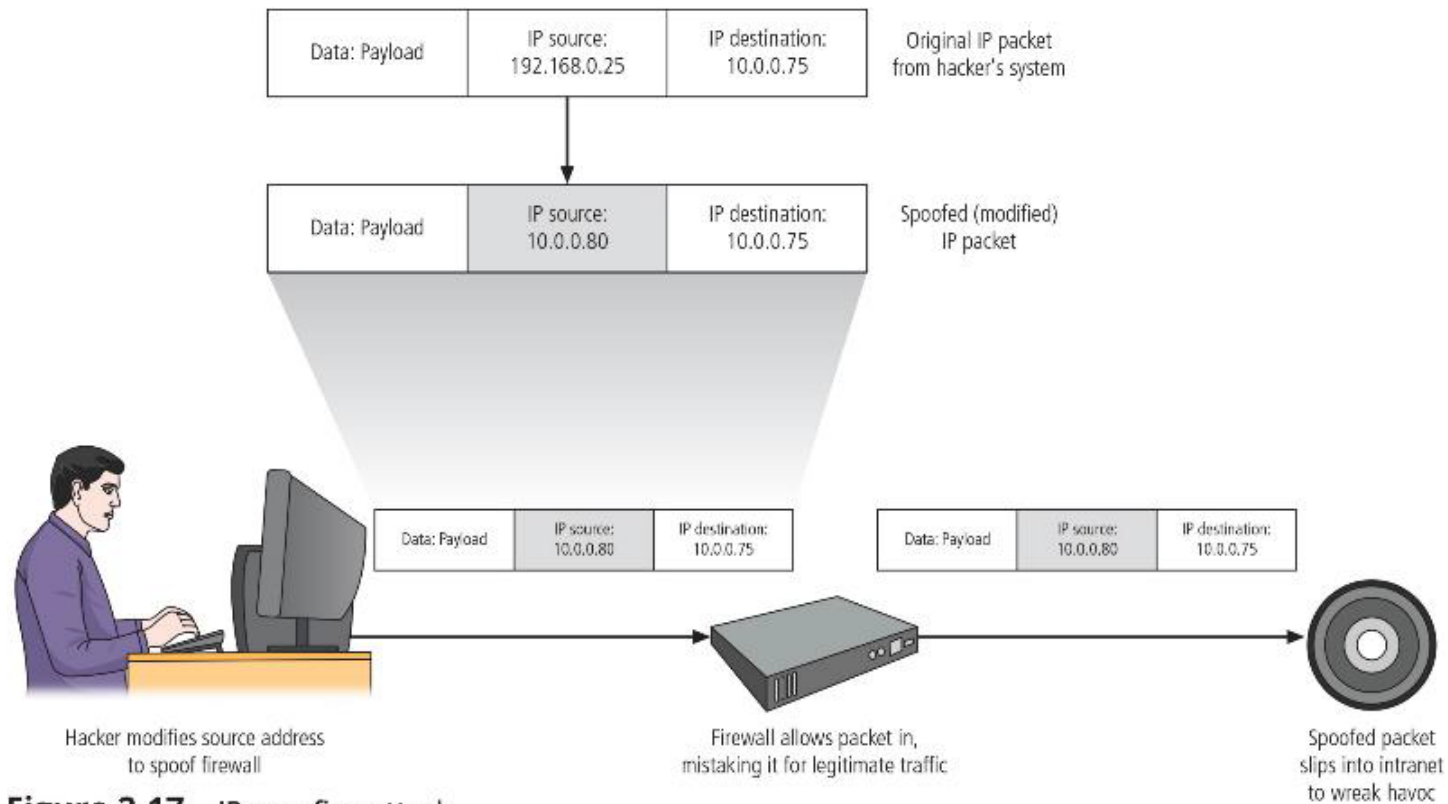


**Figure 2-17** IP spoofing attack



# Type of Software Attacks

- Types of attacks (cont'd)
  - Pharming: It attacks a browser's address bar to redirect users to an illegitimate site for the purpose of obtaining private information.
  - Man-in-the-middle: An attacker monitors the network packets, modifies them, and inserts them back into the network.

# Man-in-the-Middle Attack

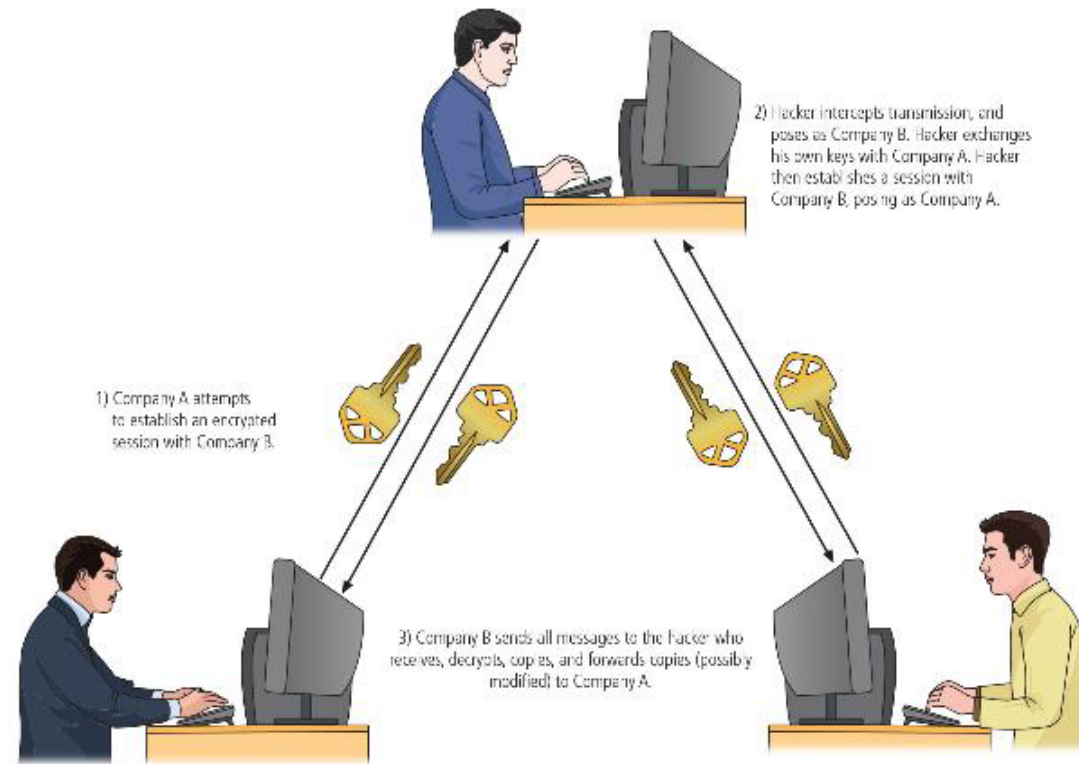


Figure 2-18 Man-in-the-middle attack



# Technical Hardware Failures or Errors

- They occur when a manufacturer distributes equipment containing a known or unknown flaw.
- They can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability.
- Some errors are terminal, while others are intermittent.
- Intel Pentium CPU failure is a notable example.
- Mean time between failure and annualised failure rates measure hardware failure rates.



# Technical Hardware Failures or Errors

- Large quantities of computer code are written, debugged, published, and sold before all bugs are detected and resolved.
- Combinations of certain software and hardware can reveal new software bugs.
- Entire Web sites are dedicated to documenting bugs.
- Open Web Application Security Project (OWASP) is dedicated to helping organisations create/operate trustworthy software and publishes a list of top security risks.

# The Deadly Sins in Software Security

- Common failures in software development:
  - SQL injection
  - Web server-related vulnerabilities (XSS, XSRF, and response splitting)
  - Web client-related vulnerability (XSS)
  - Use of magic URLs and hidden forms
  - Buffer overrun
  - Format string problems
  - Integer bugs (overflows/underflows)
  - C++ catastrophes

# The Deadly Sins in Software Security

- Common failures in software development:
  - Catching exceptions
  - Command injection
  - Failure to handle errors
  - Information leakage
  - Race conditions
  - Poor usability
  - Not updating easily
  - Executing code with too much privilege

# The Deadly Sins in Software Security

- Common failures in software development:
  - Failure to protect stored data
  - Sins of mobile code
  - Use of weak password-based systems
  - Weak random numbers
  - Using cryptography incorrectly
  - Failure to protect network traffic
  - Improper use of PKI, especially SSL
  - Trusting network name resolution
  - Neglecting change control



# Technological Obsolescence

- Antiquated/outdated infrastructure can lead to unreliable and untrustworthy systems.
- Proper managerial planning should prevent technology obsolescence.
- IT plays a large role.



# Theft

- It is the illegal taking of another's physical, electronic, or intellectual property.
- Physical theft is controlled relatively easily.
- Electronic theft is a more complex problem; the evidence of crime is not readily apparent.

# References

- Slides are devised from the recommended books:
  - Michael E. Whitman and Herbert J. Mattord, Principles of Information Security, 7th Edition.



Prifysgol Cymru  
Y Drindod Dewi Sant  
**University of Wales**  
Trinity Saint David

# Any Questions?

*Trawsnewid Addysg; Trawsnewid Bywydau*  
*Transforming Education; Transforming Lives*



[www.uwtsd.ac.uk](http://www.uwtsd.ac.uk)