CS502052 / Chapter 08

Fundamentals of Information Systems Security

Phuc H. Duong, *M.Sc.*

phuc@it.tdt.edu.vn

Textbook

- David Kim, Michael G. Solomon, [2016], *Fundamentals of Information Systems Security*, 3rd Edition, Jones & Bartlett Learning

Outline

- The Need for Information Security
- Securing Today's Information Systems
- Information Security Standards, Education, Certifications, and Laws

The Need for Information Security

Outline

- Information Systems Security
- The Internet of Things Is Changing How We Live
- Malicious Attacks, Threats, and Vulnerabilities
- The Drivers of the Information Security Business

Information Systems Security

- The Internet as we know it today is expanding rapidly as the Internet of Things (IoT) takes over and impacts our day-to-day lives
- Although the Internet officially started back in 1969, the extent to which people depend on the Internet is new
- Today, people interact with the Internet and cyberspace as part of normal day-to-day living, including personal use and business use
- Users must now address issues of privacy data security and business data security
- Security threats can come from either personal or business use of your Internet-connected device

Information Systems Security

- Intelligent and aggressive cybercriminals, terrorists, and scam artists lurk in the shadows
- Connecting your computers or devices to the Internet immediately exposes them to attack
- These attacks result in frustration and hardship. Anyone whose personal information has been stolen (called identity theft) can attest to that
- Worse, attacks on computers and networked devices are a threat to the national economy, which depends on e-commerce
- Even more important, cyberattacks threaten national security

The Internet of Things Is Changing How We Live

- It is a new topic in today's connectivity and communications vision
- This vision has many privacy, security, technical, social, and legal challenges
- The Internet first brought global connectivity
- This connectivity transformed the way people and businesses communicate
- Today, users are "always on" and always connected (i.e., hyper-connected) to the Internet

The Internet of Things Is Changing How We Live

- The IoT has **five** critical challenges to overcome:
  - Security - The Internet is already the Wild West, with plenty of bad guys and little law enforcement, yet there is an increasing demand to connect more things to the Internet.
  - Privacy - Whose data, are they? Who owns the intellectual property of personal information, data, and media? What is a privacy policy statement, and why is that important to you?
  - Interoperability - How do we define standards and protocols such that all IoT-connected devices can communicate and be accessible?

The Internet of Things Is Changing How We Live

- The IoT has **five** critical challenges to overcome:
  - Legal and regulatory compliance - The IoT vision presents legal and regulatory compliance issues that typically have not always kept pace with the speed of IoT implementations.
  - Emerging social and economic issues - The countries of the world and their citizens must quickly learn to understand and overcome any political, environmental, and economic issues presented by the IoT vision.

Malicious Attacks, Threats, and Vulnerabilities

- The Internet is an untamed new frontier
- There are many bad people wanting to steal your data
- If your device and sensitive information are connected to the Internet, there is potential for loss or damage
- Unlike in your everyday life, in cyberspace there is no real law of the land
- Criminal acts that lead to destruction and theft occur regularly
- These acts affect businesses, individuals, and governments

Malicious Attacks, Threats, and Vulnerabilities

- Malicious attacks result in billions of dollars in damages each year
- Fortunately, many companies and individuals like you are working hard to protect IT assets from attacks

The Drivers of the Information Security Business

- Information security activities directly support several common business drivers, including compliance and efforts to protect intellectual property
- Security activities can also negatively affect business drivers, making it more difficult to satisfy your business objectives

The Drivers of the Information Security Business

- Some outside requirements direct how your organization carries out its tasks
- These requirements can come from legislation, regulation, industry demands, or even your own standards
- Every organization has some requirements with which it must comply

The Drivers of the Information Security Business

- There are multiple ways that your organization can meet requirements
- Most regulations require that you develop plans to handle business interruptions or disasters
- In fact, most activities that restore operations after an interruption support several requirements
- Always consider different controls to satisfy compliance requirements
- It's important that you balance security activities with their impact on your business drivers to protect your information's security.

Securing Today's Information Systems

Outline

- Access Controls
- Security Operations and Administration
- Auditing, Testing, and Monitoring
- Risk, Response, and Recovery
- Cryptography
- Networks and Telecommunications
- Malicious Code and Activity

Access Controls

- Access controls are methods used to restrict and allow access to certain items, such as automobiles, homes, computers, and even your smartphone
- Access control is the process of protecting a resource so that it is used only by those allowed to use it
- Access controls protect a resource from unauthorized use
- Another way to define access controls is that they are mitigations put into place to protect a resource from a threat
- However you think of access controls, they are tools to make sure that only "allowed" users can access a resource

Access Controls

- Businesses use access controls to manage what employees can and cannot do
- Access controls define who users (people or computer processes) are, what users can do, which resources they can reach, and what operations they can perform
- Access control systems use several methods to achieve this goal, including passwords, hardware tokens, biometrics, and certificates
- Access can be granted to physical assets, such as buildings or rooms
- Access can also be granted to computer systems and data

Security Operations and Administration

- Security professionals must understand how security operations and administration create the foundation for a solid security program
- Security administration within an organization refers to the group of individuals responsible for planning, designing, implementing, and monitoring an organization's security plan
- Before you can form an administrative team, your organization must identify its information assets
- The administrative team then determines the sensitivity of each asset so that it can plan how to secure each one accordingly

Auditing, Testing, and Monitoring

- The purpose of a security audit is to make sure your systems and security controls work as expected
- When you review your systems, you should check for the following:
  - Are security policies sound and appropriate for the business or activity?
  - Are there controls supporting your policies?
  - Is there effective implementation and upkeep of controls?

Risk, Response, and Recovery

- Risk management is a central concern of information security
- Every action an organization takes - or fails to take - involves some degree of risk
- Attention to risk management can mean the difference between a successful business and a failing business
- That doesn't mean you eliminate every risk
- Instead, organizations should seek a balance between the utility and cost of various risk management options

Cryptography

- The algorithms, or ciphers, used to encrypt and decrypt data are collectively called a **cryptosystem**
- Most ciphers take unencrypted data, called **plaintext**, and use one or more keys to transform the plaintext into a secret message
- A **key** is a string of numbers or characters known only to the sender and/or recipient
- The resulting secret message is **ciphertext**

Cryptography

- Cryptography accomplishes four security goals:
  - Confidentiality
  - Integrity
  - Authentication
  - Nonrepudiation

Networks and Telecommunications

- Network security involves meeting an organization's essential need for network availability, integrity, and confidentiality
- The data transmitted through the network is protected from modification (either accidental or intentional), it cannot be read by unauthorized parties, and its source and destination can be verified (nonrepudiation)

Networks and Telecommunications

- Business and security requirements are as follows:
  - Access control
  - Network stability and reliability
  - Integrity
  - Availability
  - Confidentiality or nonrepudiation

Malicious Code and Activity

- Malicious code attacks all **three** information security properties:
  - **Confidentiality** - Malware can disclose your organization's private information, for instances, how spyware and Trojans, which are other forms of malware, can capture your organization's proprietary information and send it to unauthorized destinations
  - **Integrity** - Malware can modify database records, either immediately or over a period. By the time you discover the changed data, you may find that the malware has corrupted your backups as well. It is important that you verify all your data's integrity any time you suspect a security breach. The process can be expensive and is likely to be an expense you haven't budgeted for.

Malicious Code and Activity

- Malicious code attacks all **three** information security properties:
  - **Availability** - Malware can erase or overwrite files or inflict considerable damage to storage media. Some types of malware even render your information unusable without deleting or destroying it.

Information Security Standards, Education, Certifications, and Laws

Outline

- Information Security Standards
- Information Systems Security Education and Training
- Information Security Professional Certifications
- U.S. Compliance Laws

Reading

- Refer to chapter **12**, **13**, **14**, **15** in the textbook.

END OF CHAPTER