PRINCIPLES AND PRACTICES

Faculty of Information Technology, Hanoi University

Contents

I. Security Threats

II. Information Security Frameworks and Architecture

III. Pillars of Security

IV. Implementation of Information Security

V. Principles of Information Security

SECURITY THREATS

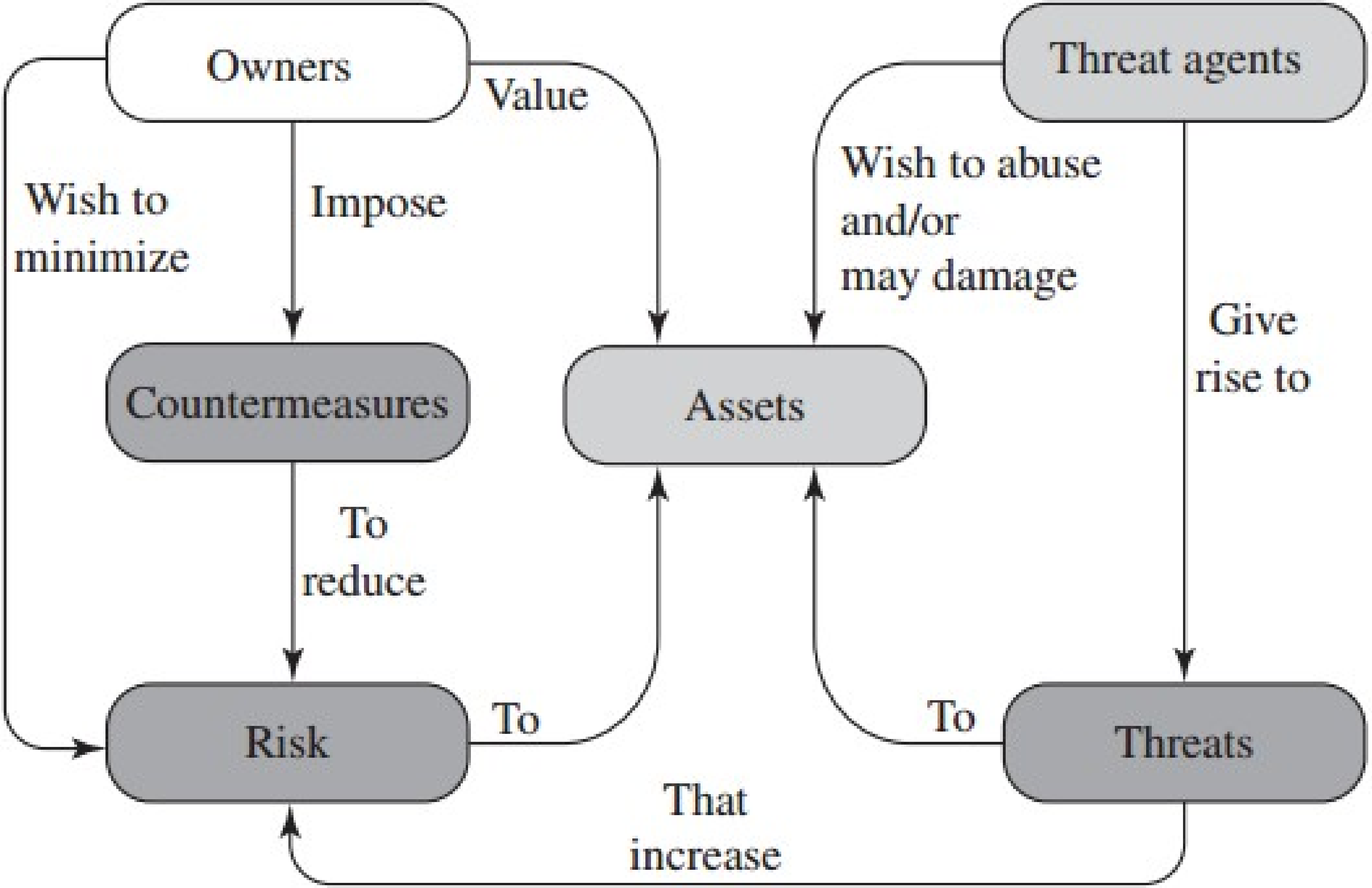

Figure 1.1 **Security Concepts and Relationships**

SECURITY THREATS - ASSETS

1. **Hardware:** Including computer systems and other data processing, data storage, and data communications devices

- A major threat to computer system hardware is the threat to availability. Theft of PC, workstation, equipment such as CD-ROMs and DVDs can lead to loss of confidentiality.
- Physical and administrative security measures are needed to deal with these threats

SECURITY THREATS - ASSETS

2. Software: Including the operating system, system utilities, and applications.

- A key threat to software is an attack on availability. Application software is often easy to be deleted. Software can also be altered or damaged to render it useless.
- Careful software configuration management, which includes making backups of the most recent version of software, can maintain high availability.
- Software modification that results in a program that still functions but that behaves differently than before, which is a threat to integrity/authenticity.
- Computer viruses and related attacks fall into this category.
- A final problem is protection against software piracy, the problem of unauthorized copying of software has not been solved.

SECURITY THREATS - ASSETS

3. Data: Including files and databases, as well as security-related data, such as password files

- Availability concerns destruction of data files, which can occur either accidentally or maliciously
- Secrecy concerns unauthorized reading of data files or databases
- Integrity concerns modifications to data files can have consequences ranging from minor to disastrous.

SECURITY THREATS - ASSETS

4. Communication facilities and networks: Local and wide area network communication links, bridges, routers, and so on

- **A passive attack** attempts to learn or make use of information from the system but does not affect system resources,

Difficult to detect because they do not involve any alteration of the data. The message traffic is sent and received in an apparently normal fashion and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern

Use encryption to prevent these attacks

- **An active attack** attempts to alter system resources or affect their operation

Involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: replay, masquerade, modification of messages, and denial of service

SECURITY THREATS - VULNERABILITY

- It can be **corrupted**, so that it does the wrong thing or gives wrong answers. For example, stored data values may differ from what they should be because they have been improperly modified.
- It can become **leaky**. For example, someone who should not have access to some or all of the information available through the network obtains such access.
- It can become **unavailable** or very slow. That is, using the system or network becomes impossible or impractical.

INFORMATION SECURITY FRAMEWORKS AND ARCHITECTURE

- Information security framework provides guidance for the effective implementation of information security in the organization and development of an effective information security architecture
- Such framework or architecture enables you to either prevent or detect and react to attacks or to recover from attacks
- To protect information and data from the above threats, organizations typically have “layers of protection.”

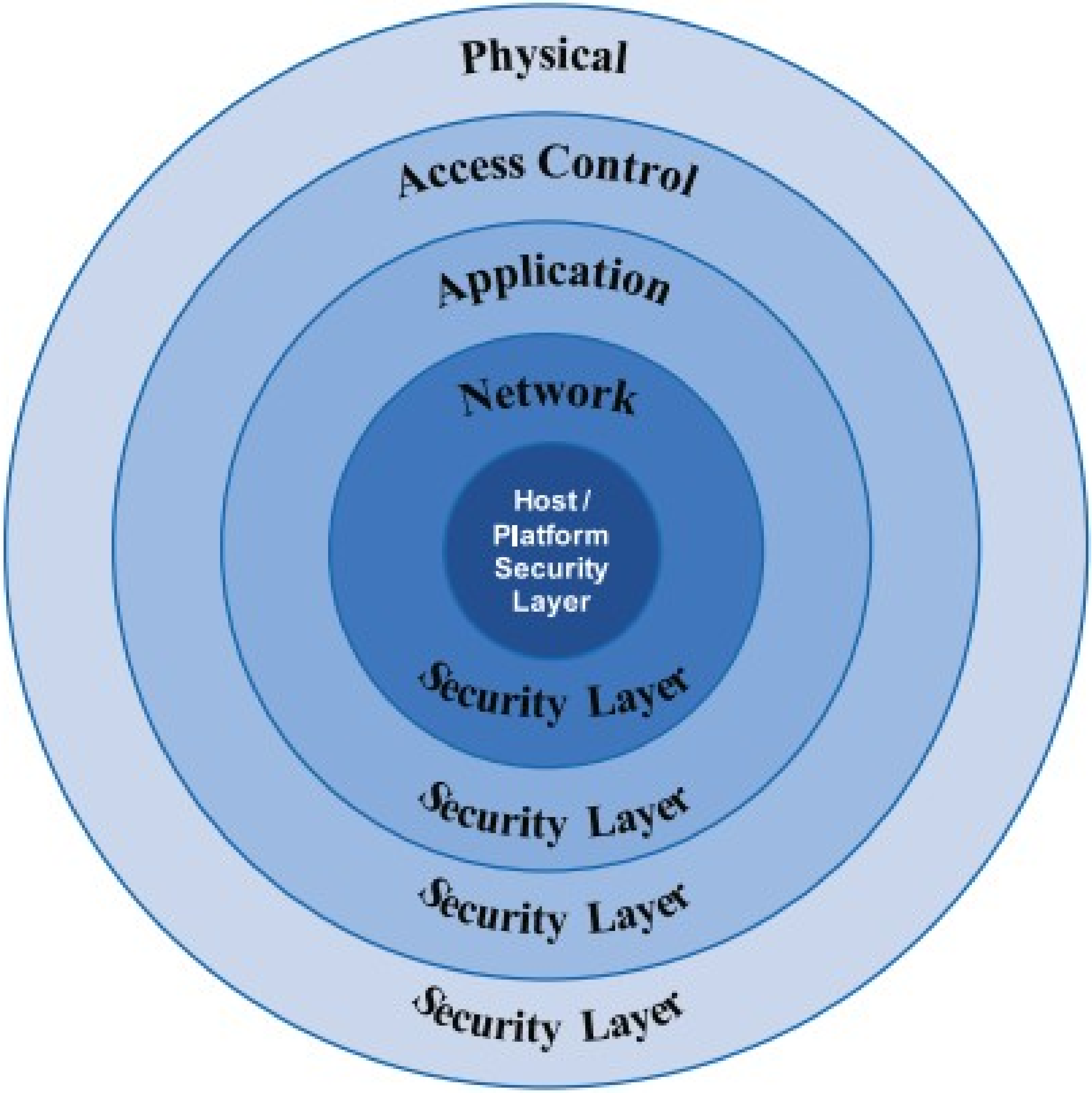

Figure 3-3. *A layered approach to security*

INFORMATION SECURITY FRAMEWORKS AND ARCHITECTURE

- The Physical security layer ensures controls like secured access, asset control, and fire protection
- The Access Control or User Layer ensures clear authentication and authorization, the security clearance through appropriate controls
- The Application security layer ensures effective controls over web servers, databases, and applications through various controls like encryption and identity management
- The Network security layer provides protection through controls like the firewall, IDS/IPS
- The Platform/Host security layer ensures controls like Host IDS/IPS, and anti-virus software

INFORMATION SECURITY FRAMEWORKS AND ARCHITECTURE

There are various Security Frameworks that are provided by various standards or models or methodologies. Some of these are

- An Information Security Management Systems Framework provided by Information Technology – security techniques – information security management systems – requirements (ISO/IEC27001:2013)supported by Information Technology – security techniques – code of practice for information security controls (ISO/IEC 27002:2013) and related standards.
- NIST Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View complemented by 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations.
- SABSA® (SABSA® is a registered trademark of The SABSA Institute which governs and co-ordinates the worldwide development of the SABSA Method.)

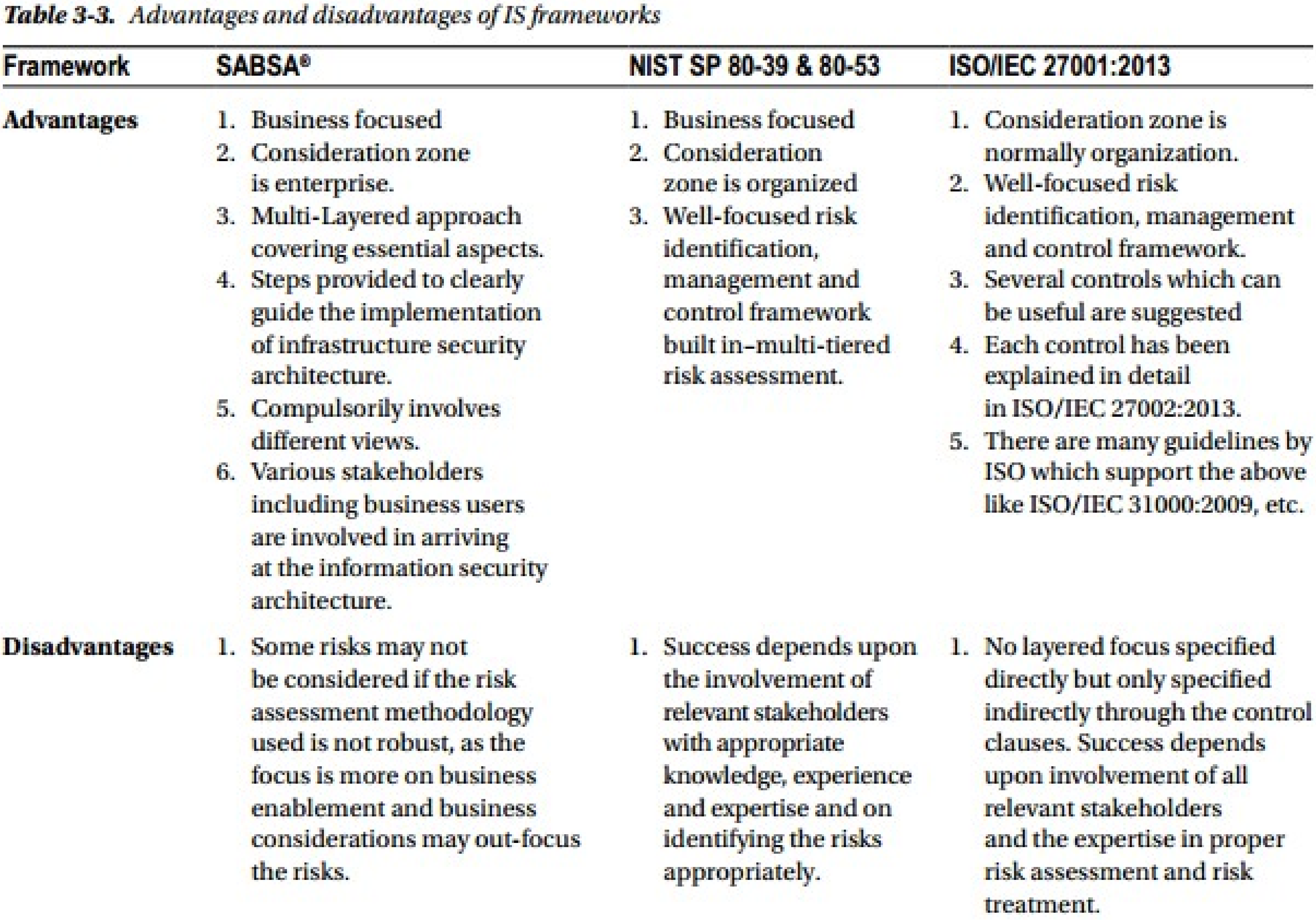

Table 3-3. Advantages and disadvantages of IS frameworks

Framework	SABSA®	NIST SP 80-39 & 80-53	ISO/IEC 27001:2013
Advantages	1. Business focused 2. Consideration zone is enterprise. 3. Multi-Layered approach covering essential aspects. 4. Steps provided to clearly guide the implementation of infrastructure security architecture. 5. Compulsorily involves different views. 6. Various stakeholders including business users are involved in arriving at the information security architecture.	1. Business focused 2. Consideration zone is organized 3. Well-focused risk identification, management and control framework built in–multi-tiered risk assessment.	1. Consideration zone is normally organization. 2. Well-focused risk identification, management and control framework. 3. Several controls which can be useful are suggested 4. Each control has been explained in detail in ISO/IEC 27002:2013. 5. There are many guidelines by ISO which support the above like ISO/IEC 31000:2009, etc.
Disadvantages	1. Some risks may not be considered if the risk assessment methodology used is not robust, as the focus is more on business enablement and business considerations may out-focus the risks.	1. Success depends upon the involvement of relevant stakeholders with appropriate knowledge, experience and expertise and on identifying the risks appropriately.	1. No layered focus specified directly but only specified indirectly through the control clauses. Success depends upon involvement of all relevant stakeholders and the expertise in proper risk assessment and risk treatment.

PILLARS OF SECURITY

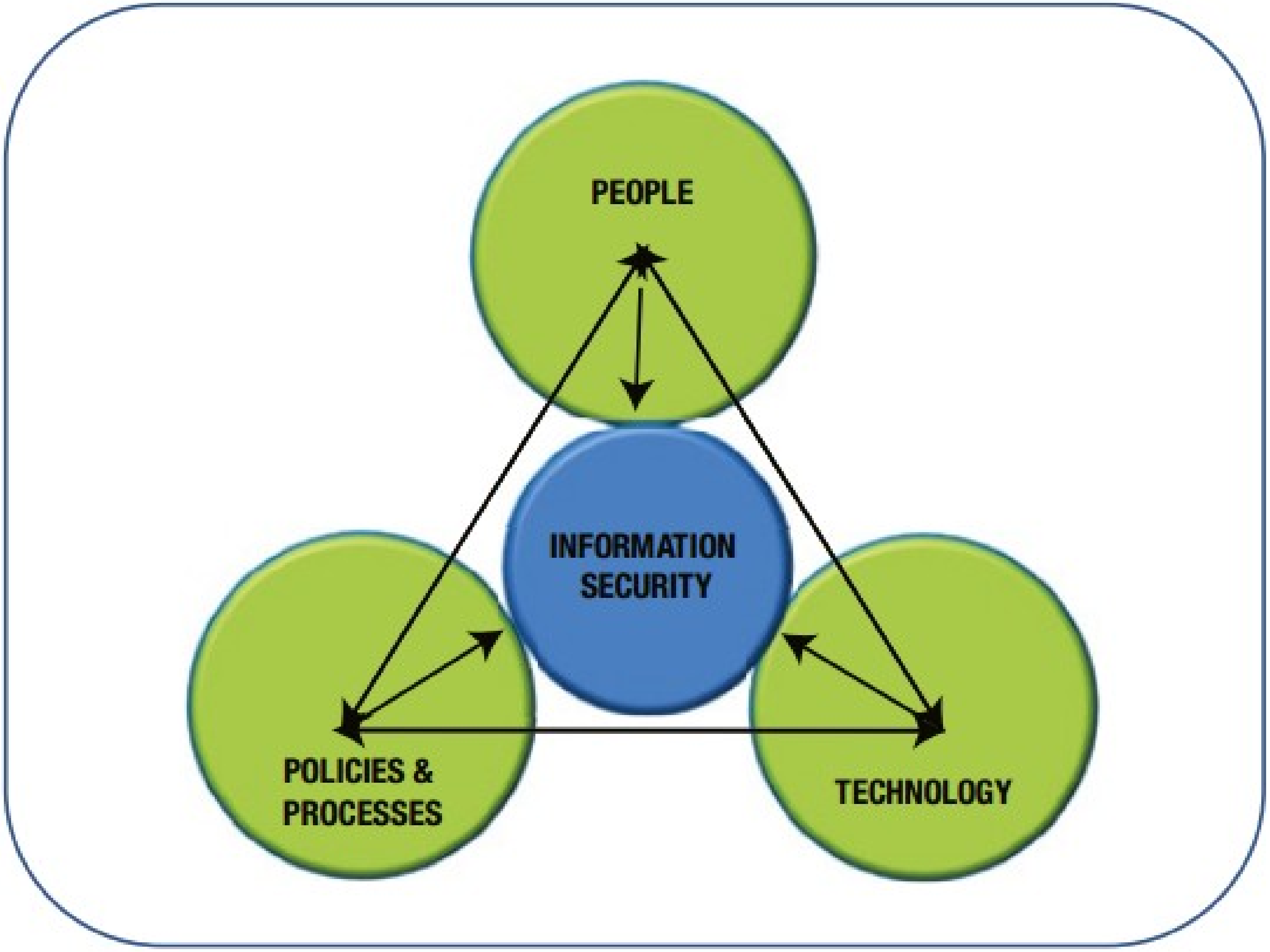

Figure 3-5. *The People, Processes, and Technology triad for information security*

PILLARS OF SECURITY

1. People:

- Strongest pillars also the weakest ones because of the lack of awareness or bad motives
- Easily prone to social engineering attacks or other malicious attacks.

2. Organization of Information Security

- Everybody needs to involve: receptionists, security staff, housekeeping staff, top managers…
- Requires commitment from all levels of an organization to ensure the effectiveness of information security
- Plan and implement information security to protect the organization, customers, partners, suppliers, and other relevant stakeholders

PILLARS OF SECURITY

3. Policies, Procedures, and Processes

- Describe how the intent of the policies is to be implemented
- Detail step-by-step instructions on how to carry on the work so that the intentions of these policies are adhered to
- Need to be reviewed and kept current
- Training is a must, and should be ongoing and continual
- Information security is incomplete without clearly defined policies
- Policies provide guidance to everyone and depict the commitment of management to them.
- Some of the policies that are important to most of the organizations:

PILLARS OF SECURITY

- Information Security Management Systems Policy
- Access Control Policy
- Information Classification and Handling Policy
- Physical and Environmental Security Policy
- Acceptable Use of Assets Policy
- Clear Desk and Clear Screen Policy
- Privacy and Protection of Personally Identifiable Information Policy
- Mobile Devices and Teleworking Policy
- Backup Policy
- Restrictions on Software Installations and Use Policy

PILLARS OF SECURITY

- Protection from Malware Policy
- Management of Technical Vulnerabilities Policy
- Information Transfer Policy
- Communications Security Policy
- Cryptographic Controls Policy
- Policy on Supplier Relationships

4. Technology

- Should fulfil the requirement of information security architecture
- Auto monitoring and alerting systems, logging systems, detecting systems, preventive systems, and recovery systems. Examples are firewalls, IDS/IPS, and anti-virus software

IMPLEMENTATION OF INFORMATION SECURITY

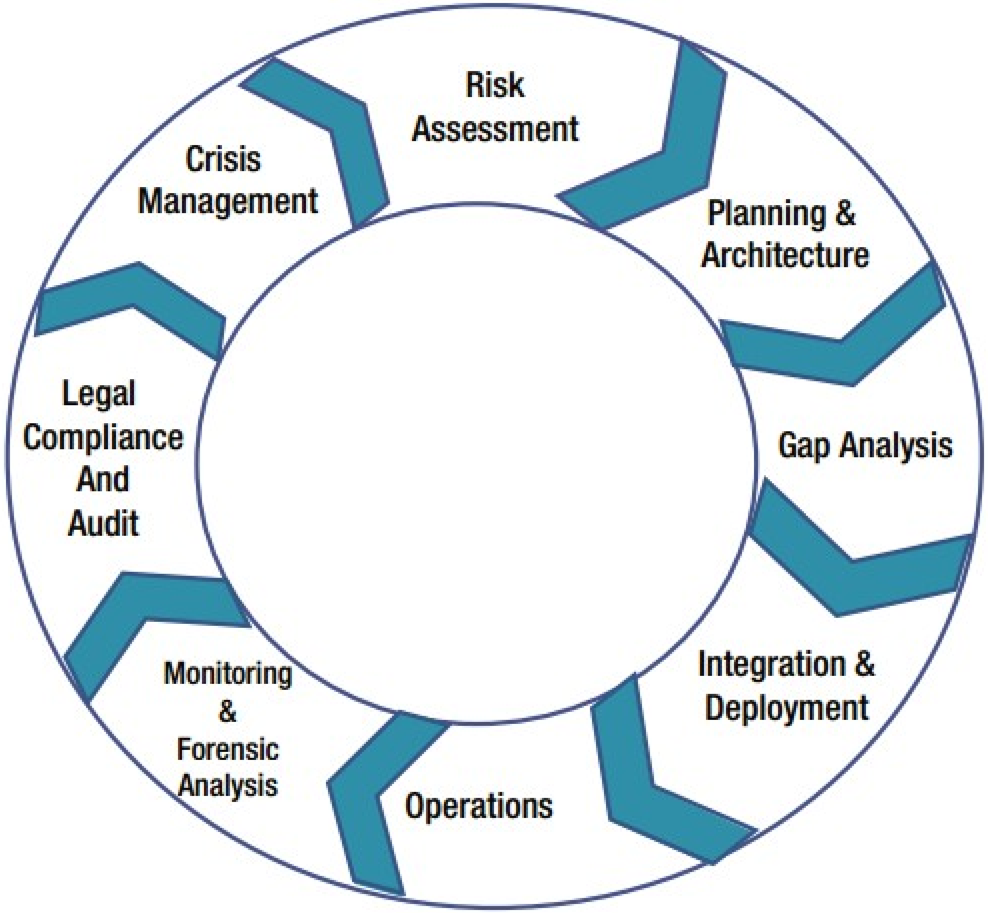

Figure 3-9. *The implementation cycle of information security*

IMPLEMENTATION OF INFORMATION SECURITY

1. Risk assessment

- Vulnerabilities and threats to information assets even from

the outside world

2. Planning and Architecture

- Identify the owners for various activities, roles, and responsibilities
- Schedules used also clearly depicts the timelines
- The steps planned depend upon the methodology or framework used
- Effective information security infrastructure or architecture provides ease of use and generates confidence to all the stakeholders including business users

IMPLEMENTATION OF INFORMATION SECURITY

3. Gap analysis

- Ensures a check on the implementation of the policies, procedures, and processes, as well as the effectiveness of the existing protective mechanisms or controls including the effectiveness of the information security architecture
- May be done through periodical risk re-assessments leading to additional controls to be implemented through new risk treatment plans

IMPLEMENTATION OF INFORMATION SECURITY

4. Integration and deployment

- An integrated view at all times in the totality of the business and the organization is required
- Effective deployment of all intended policies, procedures, and processes, along with the intended implementation of information security architecture and its various layers is required
- Incomplete implementation or inadequate attention to any one of the layers may defeat the controls built in other layers.
- Relevant people need to be trained, and tools, if any, need to be configured appropriately. The correct working of such tools should be confirmed by testing as required and defects, if any, have to be fixed or their impact understood and only then these tools have to be used.

IMPLEMENTATION OF INFORMATION SECURITY

5. Operations

- Information security should not be ignored in day-to-day operations
- It should be an integral part of all the activities.
- Operations need to be carried out strictly according to the established policies, procedures, and processes
- Any violation to speed up the activities or ignorance can lead to serious consequences
- Example: Not checking the backup media through periodical restoration may lead to the tape being not readable or restorable when required, or backups were not taken because the system administrators were busy on another activity

IMPLEMENTATION OF INFORMATION SECURITY

6. Monitoring and Forensic Analysis

- Any organization needs to keep monitoring the threats to it so that it can react to the threats effectively and on time
- For example, to find out about all the intruder activities manually through logs is a humungous activity. There are many tools available to monitor, filter, detect, and/or to correct and alert on such aspects such as: firewalls and IDS/IPS. Even simple things like disk space monitoring and bandwidth usage monitoring, if not done on a timely basis, may lead to systems not being usable or available
- Sometimes the forensic analysis (where the causes may not be obvious or straight forward) may have to be carried out

IMPLEMENTATION OF INFORMATION SECURITY

7. Legal compliance and audit

- One of the biggest threats to an organization’s existence is non-compliance to legal requirements
- Organizations can be permanently shut down if the non-compliance is severe.
- There are a lot of laws enacted to prevent the misuse of information technology which may require special skills to understand the compliance in the context of information technology
- Hence, periodic audits by knowledgeable independent or internal experts will help the organizations

IMPLEMENTATION OF INFORMATION SECURITY

8. Crisis management

- The Crisis Management Plan, Business Continuity Plan, or Disaster Recovery Plan are interchangeably used to denote a single entity
- Organizations can face crisis because of natural disasters, mistakes of employees, senior management, or because of the external attacks like the attacks from the hackers.
- Organizations need to respond effectively and also restore their business back to normalcy after such attacks
- a well-planned business continuity and crisis management plan should be put in place
- Disaster recovery and business continuity should become an integral part

Principles of Information Security

Principle 1: Computer Security Supports the Mission of the Organization

As we have seen, every organization has objectives to achieve, whether they are business goals or social goals. Any other system is rendered useless, whether it be information technology system or procedures or otherwise, if it does not enable the achievement of these primary objectives of the organization in conjunction with the goals of these systems too.

Principles of Information Security

Principle 2: Computer Security is an Integral Element of Sound Management

This principle is straight forward and it cannot be more relevant than in today's world. In today's well connected world, where the attacks can happen on any system from any other part of the world and nobody can be absolutely sure of the protection put in place, information security can be ignored only at the peril of an organization.

Principles of Information Security

Principle 3: Computer Security Should Be Cost-Effective

At the end of the day, every organization has to sustain, continue to sustain, and grow its business and profitability. Even organizations with social objectives have limited funding available to them and the expectation is that they use it judiciously. Hence, just because an excellent security system is available in the market, one should not go ahead with it unless the benefits accrued by its usage are far more than the costs of their purchase and implementation. This is one of the fundamental requirements for any organization of any size in any business.

Principles of Information Security

Principle 4: Systems Owners Have Security Responsibilities Outside Their Own Organization

Today, in the era of the Internet and web applications, many of the systems are used by users, whether employees or customers, from outside the organizational physical boundaries. Every individual has the right to be assured that the system or applications that she/he is using is secure. It is the organization’s responsibility to ensure that safety is built into these applications and their users are duly assured of the security in them. No organization can shirk its responsibility in this regard as the growth of business, in recent times, depends on new tools of doing business.

Principles of Information Security

Principle 5: Computer Security Responsibilities and Accountability Should Be Made Explicit

Having clarity is what makes the difference when it comes to achievement. As we have seen, decisions are not made by the people who are normally working with the data because the authorities are not clearly defined and assigned. Such a state of confusion can lead to disasters in organizations today, as computer security incidents or breaches and disasters on account of them have to be dealt with using speed, precision, and clarity.

Principles of Information Security

Principle 6: Computer Security Requires a Comprehensive and Integrated Approach

Most of the organizations operate in a highly competitive environment. For their efficiency and effectiveness, all aspects of business, business enablers and business protection systems have to work in perfect harmony and need to complement and supplement each other seamlessly into a comprehensive and integrated approach. This is what we emphasized throughout our discussions in this chapter, including in the context of information security frameworks / architecture.

Principles of Information Security

Principle 7: Computer Security Should Be Periodically Reassessed

As we discussed earlier, changes are the only constant in this world. In the changing context, we need to navigate in the right direction. In order to check for our direction and do course corrections, we need to do periodical reassessment of the organizational computer security. We have already discussed the benefits of the periodical gap analysis through periodical risk assessment as a means of course correction.

Principles of Information Security

Principle 8: Computer Security is Constrained by Societal Factors

It is true that there is a possibility of conflict between information security requirements and societal factors, e.g. logging activities and privacy requirements. While each of them has significance of their own, we need to ensure a balance between these. The balancing depends upon the context and expectations. It is possible that under certain circumstances, one can complement and support the other.

Summary

I. Security Threats

II. Information Security Frameworks and Architecture

III. Pillars of Security

IV. Implementation of Information Security

V. Principles of Information Security

Q & A