CHAPTER 3

Key Concepts and Principles

Introduction

Every organization or enterprise exists to achieve its objectives, both business objectives and social objectives. Its existence or continued existence is of no use unless it is able to achieve its objectives. For the continued existence of any organization, information security has become a non-negotiable necessity. However, the acceptability for information security is very low in an organization because of its arbitrary implementation. Information security will be appreciated by everybody if it is implemented, keeping in mind an organization's business objectives and business requirements. Furthermore, information technology has to enable information security which, in turn, will protect its business, customers, partners, and systems, such as its people, infrastructure (including its networks), and applications. This in turn means that all the strategies of the organization – business strategies, IT strategies, and information security strategies – have to complement each other and are to be balanced.

Information security refers to the processes and methodologies that are designed to protect sensitive information or data from unauthorized access, use and misuse, disclosure, modification, destruction, or disruption. In addition, it also covers the validity or genuineness of the information and rejection of false information received from others. The terms "information security," "computer security," "data security," and "information assurance" are frequently used interchangeably. Though there are subtle differences between these different terms, their common goal is to protect the Confidentiality, Integrity, and Availability (CIA) of data.

The objective of information security is to protect information and its critical assets including people, systems, and hardware that use or process, store, and transmit the data. To protect the information and its related systems, organizations have technology and tools, policies and processes, and also the necessary training and awareness programs, and also rewards for abiding by the security policies and processes and penalties for any security breaches. Many organizations have disciplinary processes instituted that consider and investigate the security breaches. Intentional security breaches normally lead to the termination of the employee / contractor or disengagement of the supplier. Unintentional or accidental security breaches may be considered leniently but organizations should still warn the employees in such cases. Reporting of the security breaches or incidents is appreciated by many organizations and is rewarded in kind or cash.

The requirements of information security have undergone major changes in the last few decades. Before the widespread use of computers and the Internet, information security was primarily restricted to physical access, such as a guarded room and locked security cabinets to store sensitive confidential information. With technological innovations and the introduction of computers and TCP/IP communication, automated tools became a necessity for protecting data stored on a computer system. The need for computer security became even more evident with the advent of the Internet where the systems and data are accessed and transmitted over the public telephone and data network. **Physical Security** is still a significant part of any security system and cannot be ignored as it is an important line of defense for most organizations. **Hardware Security** can be primarily considered under Physical Security, even though some of the components of the hardware can be considered under other securities such as Network Security.

TCP/IP is the underlying protocol for computer communication that facilitates distributed connectivity and communication facilities for sharing data between two computers present at different locations. TCP/IP is the underlying protocol that resulted in the invention of the Internet and the World Wide Web (WWW). As information

is now being shared by millions of users on the Internet, **Network Security** became extremely essential to protect the data that is being transmitted and guarantee that the data is not tampered with during the transmission. **Communications Security,** that is, securing communications through the use of various mechanisms, can be considered broadly as a part of Network Security. Secure routing mechanisms, secure session mechanisms, and secure encryption mechanisms may be considered as part of Communications Security.

Another important layer of security is **Software Security**, which broadly deals with the Operating System Security, the Application Security, and the security of software utilities/tools, including the security of tools used to provide information security. Operating systems provide many of the functionalities required for the servers and computers to work effectively, including communication capabilities with other systems, processing of information, and effective functioning of applications. Recently, with the increased use of mobile phones and tablets (which are also used for significant official work) and with such diverse operating systems like Android, iOS, Symbian, and BlackBerry, many more possible security issues have opened up. Recent years have also seen a huge growth in the number of applications developed and deployed on these products. It is not yet clear to what extent secure practices are being used during their design, development, and deployment. As seen in practice, secure design, development, and deployment is lagging behind significantly, even on stable and best in class operating systems, thus opening up several avenues for security flaws and providing entry points for malicious attackers. This may also provide unintended entry points for the insiders with malicious intent.

Human or personnel security is another important layer. Keeping personnel motivated, making them aware of the information security risks, and involving them in the implementation of the same is an important aspect of information security which cannot be forgotten at any cost. Employees (permanent or temporary), contractors, and suppliers are all significant in this regard.

All of the important layers that have been discussed (supported by policies, procedures, and processes to plan, implement, monitor, audit, detect, correct, and change of any of the components of all the above layers) constitute a layered approach to information security. Appropriate coordination between the various layers, and the distribution of risks and opportunities to different layers, will vary, depending on the cost effectiveness and ease of use, and the impact on the efficiency and effectiveness of information security.

Figure 3-1 illustrates the context diagram of various layers of information security interacting with each other and providing a robust security architecture.

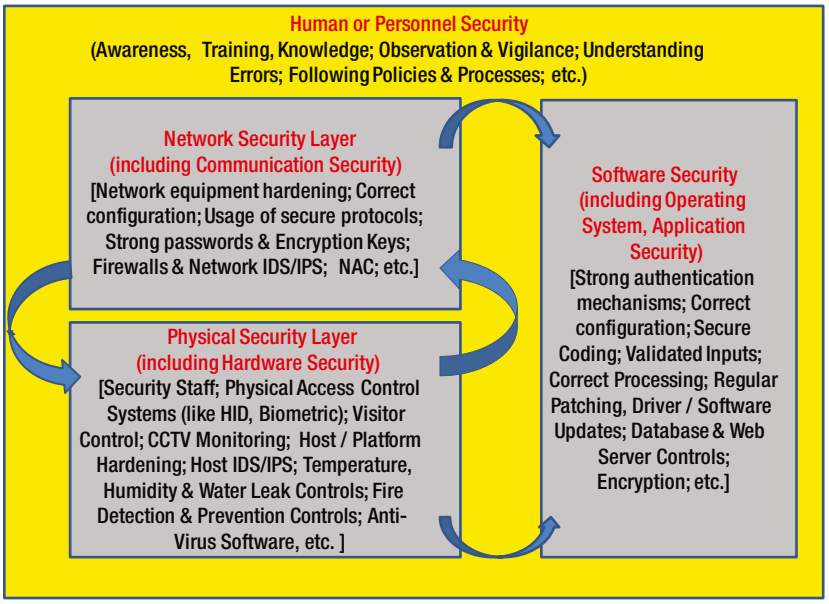

Figure 3-1. *Primary layers of information security*

An effective Information Security Architecture should consider all the layers without omitting any of them. It should also consider the effectiveness and have an integrated view of all of them, rather than a secluded and narrow view of any one business, unit, equipment, component, tool, or utility. Before beginning the discussion of an effective Information Security Architecture, we will look into various threats that are normally considered under these layers.

Security Threats

The word 'threat' in information security means anyone or anything that poses danger to the information, the computing resources, users, or data. The threat can be from 'insiders' who are within the organization, or from outsiders who are outside the organization. Studies show that 80% of security incidents are coming from insiders.

Security threats can be categorized in many ways. One of the important ways they are categorized is on the basis of the "origin of threat," namely external threats and internal threats. The same threats can be categorized based on the layers described above.

External and Internal Threats

External threats originate from outside the organization, primarily from the environment in which the organization operates. These threats may be primarily physical threats, socio-economic threats specific to the country like a country's current social and economic situation, network security threats, communication threats, human threats like threats from hackers, software threats, and legal threats. Social engineering threats like using social engineering sites to gather data and impersonate people for the purpose of defrauding them and obtaining their credentials for unauthorized access is increasing. Theft of personal identifiable information, confidential strategies, and intellectual properties of the organization are other important threats. Some of these physical threats or legal threats may endanger an entire organization completely. Comparatively, other threats may affect an organization partially or for a limited period of time and may be overcome relatively easily. Cybercrimes are exposing the organizations to legal risks too.

Some of the important external threats are illustrated below in Figure 3-2.

Figure 3-2. *External threats*

Internal threats originate from within the organization. The primary contributors to internal threats are employees, contractors, or suppliers to whom work is outsourced. The major threats are frauds, misuse of information, and/or destruction of information. Many internal threats primarily originate for the following reasons:

- Weak Security Policies, including:
  - Unclassified or improperly classified information, leading to the divulgence or unintended sharing of confidential information with others, particularly outsiders.
  - Inappropriately defined or implemented authentication or authorization, leading to unauthorized or inappropriate access.
  - Undefined or inappropriate access to customer resources or contractors/suppliers, leading to fraud, misuse of information, or theft.
  - Unclearly defined roles and responsibilities, leading to no lack of ownership and misuse of such situations.
  - Inadequate segregation of duties, leading to fraud or misuse.
  - Unclearly delineated hierarchy of "gatekeepers" who are related to information security, leading to assumed identities.

- Weak Security Administration, including:
  - Weak administrative passwords being misused to steal data or compromise the systems.
  - Weak user passwords allowed in the system and applications, leading to unauthorized access and information misuse.
  - Inappropriately configured systems and applications, leading to errors, wrong processing, or corruption of data.
  - Non-restricted administrative access on the local machines and/or network, leading to misuse of the system or infection of the systems.
  - Non-restricted access to external media such as USB or personal devices, leading to theft of data or infection of the systems.
  - Non-restricted access to employees through personal devices or from unauthenticated networks and the like, leading to data theft.
  - Unrestricted access to contractors and suppliers leading to theft or misuse of information including through dumpster diving or shoulder surfing.
  - Unrestricted website surfing, leading to infections of viruses, phishing, or other malware.
  - Unrestricted software downloads leading to infection, copyright violations, or software piracy.
  - Unrestricted remote access leading to unauthorized access or information theft.
  - Accidentally deleting data permanently.
- Lack of user security awareness, including:
  - Identity theft and unauthorized access due to weak password complexity.
  - Not following company policies, such as appropriate use of assets, clean desk policy, or clear screen policy, leading to virus attacks or confidential information leakage.
  - Divulging user IDs and/or passwords to others, leading to confidential information leakage.
  - Falling prey to social engineering attacks.
  - Falling prey to phishing and similar attacks.
  - Downloading unwanted software, applications, or images or utilities/tools leading to malware, viruses, worms, or Trojan attacks.
  - Improper e-mail handling/forwarding leading to the loss of reputation or legal violations.
  - Improper use of utilities like messengers or Skype and unauthorized divulgence of information to others.
  - Inappropriate configuration or relaxation of security configurations, leading to exploitation of the systems.
  - Entering incorrect information by oversight and not checking it again or processing the wrong information.
  - Ignoring security errors and still continuing with transactions, leading to the organization being defrauded.

Some of the important external and internal threats are collated in Table 3-1 for easy reference.

Table 3-1. *External and internal threats*

External Threats	Internal Threats
Physical Threats	**Human Threats**
Natural disasters like cyclones, hurricanes, floods, earthquakes, etc.	Frauds, misuse of assets or information
Fire	Errors or mistakes by the employees
Terrorist threats like bombs, hostage situation	Espionage, Shoulder surfing
Hardware destruction	Social Engineering by the employees
Physical intrusion	Exploitation of lack of knowledge or ignorance of fellow employees
Sabotage	Use of weak administrator passwords or passwords of others and gaining unauthorized access
Theft of the assets and Intellectual Property sensitive assets/information	Theft
Network Threats	Policies not executed or followed
Sniffing or Eavesdropping	Improper segregation of duties leading to fraud or misuse
TCP/IP issues like snooping, authentication attacks, connection hijacking	Malware infection threats due to infected media usage or unauthorized software downloads
Spoofing	**Internal Application Issues**
Man in the middle attack	Invalidated inputs
Denial of service attacks	Misconfigured application leading to errors or wrong processing
SQL injection	Inappropriate error or exception handling leading to issues
Exploitation of default passwords on network equipment being unchanged	Parameter manipulations; Manipulation of Buffer Overflows
Exploitation of weak encryption	Unauthorized access
Software Issues	**Other Issues**
Defects leading to errors	Unrestricted access to USB leading to pilferage of information
Defects being exploited	System or data corruption may be due to power surges, temperature control failure or for other reasons
Malware like Viruses, Worms, Trojans, Back doors	Hardware failure due to malfunctioning
Bots or Botnets	Infrastructure like UPS failure due to improper maintenance
Invalidated inputs	
Authentication attacks	
Exploitation of misconfigurations	

(*continued*)

Table 3-1. (*continued*)

External Threats	Internal Threats
Session Management related issues	
Inappropriate error handling or exception handling by the applications	
Buffer overflow issues	
Cryptography wrongly handled by applications	
Parameter manipulations	
Operating system related issues – security flaws in the operating system	
Human Threats	
Social engineering	
Attack by hackers/man in the middle	
Blackmail, extortion	
Espionage	
Compliance Threats	

Note: The legal requirements pertaining to information and communication can lead to closure of the organization or huge penalties

Information Security Frameworks and Information Security Architecture

Information security framework provides guidance for the effective implementation of information security in the organization and development of an effective information security architecture, which in turn, provides assurance that information security has been effectively employed in the organization. One word of caution here: "Whatever the level of implementation, you cannot be 100% assured of information security". However, if you have implemented security measures effectively, this will enable you to control many of the security threats and prepare you to be quick in providing reactive responses to the threats. Organizations can only be defensive in their approach as an offensive strategy is illegal. Such framework or architecture enables you to either prevent or detect and react to attacks or to recover from attacks.

In order to protect information and data from the above threats, organizations typically have "layers of protection." This practice of layering defenses improves an organization's overall security posture. Successful organizations have layers of security, as shown in the Figure 3-3.

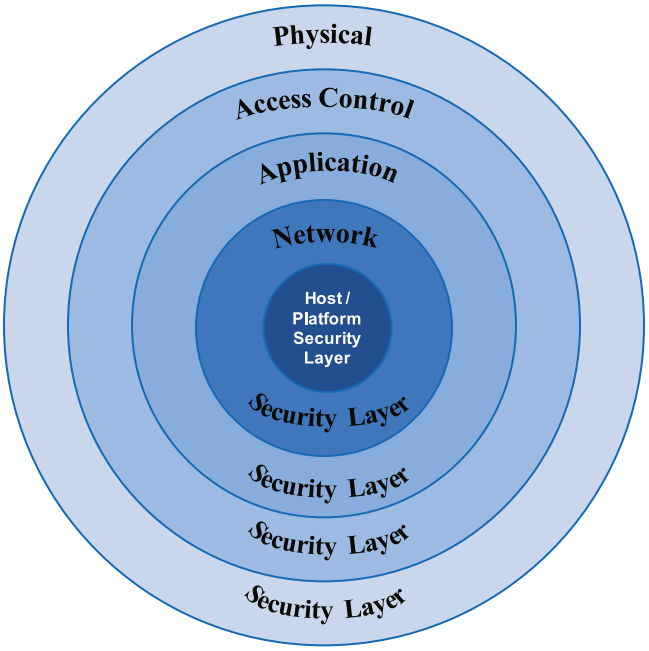

Figure 3-3. *A layered approach to security*

As you can see in Figure 3-3, these five layers of security support and complement each other. While the Access 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 while the Platform/Host security layer ensures controls like Host IDS/IPS, and anti-virus software, whereas the Physical security layer ensures controls like secured access, asset control, and fire protection.

The Platform/Host Security is ensured primarily through the hardening of the servers. Root / administrator passwords are changed from the default passwords to strong passwords and are tightly controlled. Furthermore, the anti-virus solutions of repute when installed on the servers provide significant protection for them from malware or spyware infections. Security patches are released by most of the operating system vendors periodically. The timely application of these to the concerned server after testing the impact of them on the applications working on such platforms/hosts ensures that these servers are well protected. Similarly, drivers need to be maintained and updated as needed. Periodic preventive maintenance of these hosts to clean up space, remove unwanted files, archive unwanted data, defragment disks, ensure up-to-date and relevant patch updates, and software or driver upgrades, will ensure continued performance. Otherwise, there may be a performance degrade which impacts availability and increases security threats. Similarly, the maintenance of facilities and utilities, such as temperature controls in the server room/data center, humidity controls in the server room/data center, and preventive maintenance of UPS, help ensure secure systems. Weak administrator passwords can also put the servers at risk.

As we saw earlier in this chapter, network security is the next protective layer that connects the hosts/platforms to others. Some aspects that need to be ensured here are that the network equipment is hardened, default passwords are invariably replaced with stronger passwords, all the network equipment such as routers are configured correctly, and protocols are used appropriately depending upon the infrastructure and organizational needs. Firewalls and IDS/IPS need to be set up appropriately with relevant configurations and policies so that they are able to detect, alert, or prevent some of the attacks. Weak administrator passwords, weak or unprotected encryption keys, or misconfigurations can be exploited and can place the organizations and its business at risk. Networks are prone to other types of attacks such as spoofing, man in the middle attacks, sniffing, or eavesdropping, leading to

impersonation or loss or misuse of data. Networks are also prone to such vulnerabilities like session hijacking and denial of service attacks.

Application security is a major issue worldwide. Web servers and databases need to be secured by appropriate installations and configurations. In this fast-paced world, the focus on completion of software development and its delivery has become more important than its security. Surprisingly, most of these applications are not tested for security. These applications can be prone to attacks like SQL injection, buffer overflows, and invalidated data inputs which can eventually lead to the compromise of the host systems on which they are running. Similarly, ineffectively tested or misconfigured applications may lead to processing errors or not validating the errors, leading to the loss of integrity of the data. Weak authentication and authorization mechanisms built into these applications or misconfiguration of these applications may lead to unauthorized access or other issues like corruption of data and the like. Defects in applications can not only lead to errors in data but such defects related to security can lead to security breaches. Applications not patched on a timely basis may be prone to viruses or the exploitation of such security flaws or errors. It is also possible that the interface between two applications is weak, which leads to an insecure transfer of data between these applications, and subsequent exposure of this data to others.

Access to systems is regulated by the access control layer. Access control layers have to be set up as per the organization's access control policy. Some of the access control models of interest are mandatory access control, discretionary access control, and non-discretionary access control models. Some of the access control administration models are the centralized administration model, decentralized administration model, and the hybrid administration model. Both the internal and external access controls and external need to be appropriately handled. Authentications and authorizations have to be set up appropriately. Primary threats due to an improperly configured access layer are unauthorized or have incorrect access or denial of appropriate access. Over time, it has been observed that single authentication mechanisms are broken relatively easily, making multiple authentications preferable for maximum security.

The other important layer is the physical security layer. Traditionally, security guards and locks were the primary means of physical security. Because of the human element involved where negligence or ignorance lead to security threats, complementary security controls like biometric access (finger prints, iris scan, etc.), access through smart cards coupled with passcodes, and the like, are implemented. Selection of an appropriate location for the organization protects it from potential natural hazards like floods. Having secured electrical wiring with the appropriate safety mechanisms like well-maintained earth pits, UPS for regulated power, trippers, and fuses provides substantial security from electrical fires. Good practices like not storing flammables like diesel, petrol, other chemicals in the premises, and not storing easily flammable materials like empty cartons or huge quantities of old papers reduce the threats of fire. Proper visitor control mechanisms and control over the entry and exit points can reduce the propensity for physical intrusion or unauthorized physical access or sabotage, vandalism, espionage, theft, and destruction of systems. Policies not followed by employees can allow such threats due to tailgating which is a very common issue at most organizations. Ignorance and incompetence, and a lack of awareness and training can lead to mistakes.

Layers of security provide complementary controls which mean that a threat not controlled by one layer is controlled by other layer and vice versa. Some of the threats may be controlled by multiple layers also. Thus, a layered approach, which is an integrated approach, provides better protection to the organization than a single layered approach. The controls built through the layered approach normally defend the organization against most threats. This effectively means that the threat has to percolate multiple layers before it is effective.

"Defense-in-depth" builds over a layered security approach and complements it through additional mechanisms, especially for monitoring, alerting, and emergency response, including disaster recovery, as applicable. This normally includes forensic analysis and criminal activity reporting. This is also complemented where required by authorized personnel activity auditing.[1] Normally, the defense-in-depth strategy monitors current activities, and alerts you to imminent threats, thus enabling you to counter such threats through an emergency response or quick recovery, whereas multi-layered security control strategy delays the threat and provides ample time to react. For defense-in-depth to be effective at monitoring the speed at which the traffic/data is monitored and analyzed, and for the alerts to be communicated to the relevant tools or experts for further action, the analysis should be very high for such emergency responses to be effective.[1] Furthermore, such tools should have the capability to provide zero or very limited false alerts. Also, a team of experts like the Computer Emergency Response Team (CERT) should be formed and trained to handle such alerts and deal with emergency responses. Sometimes, it is impossible to avoid or counter an attack, but alerts need to be investigated immediately. This requires a forensic analysis capability in the organization. As organizations cannot carry out a counter-offensive in response to an attack because of legal restrictions,

particularly in the case of such attacks where the solution is not immediately known, it is advisable to involve agencies like internet service providers or government security agencies (as appropriate to the gravity of the situation) so that the appropriate responses or corrective mechanisms may be identified and implemented at the earliest possible time.

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/IEC 27001:2013) 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.)

None of them use the same layers, but all have core layering concepts in common either depicted directly or indirectly through means such as the control objectives.

Information Security Management Systems Framework Provided by ISO/IEC 27001:2013

The framework suggested in this standard, i.e., information technology, security techniques, information security management systems, and requirements (ISO/IEC 27001:2013) is complemented by the guidance provided in the code of practice for information security controls (ISO/IEC 27002:2013).[2] This standard suggests that the security issues related to an organization have to be understood both in external and internal contexts and based on the needs and expectations of the interested parties. A risk assessment is necessary whereby the level of a risk is understood, the quantified risk has to be compared with acceptable risk as per the acceptance criteria of an organization and where appropriate, risk treatment options have to be identified, planned, and enacted.[2] The standard does not dictate any specific risk assessment methodology to be used. Where risks need to be mitigated, additional controls can be identified from various sources or from the list of controls provided in the standard.[2]

This standard 27001:2013 does not suggest any specific layers or a layered approach, but it provides guidance as to various structural elements for an effective information security implementation, through control clauses. The control clauses are Information Security Policies, Organization of Information Security, Human Resources Security, Asset Management, Access Control, Cryptographic Controls, Physical and Environmental Security, Operations Security, Communications Security, System Acquisition, Development and Maintenance, Supplier Relationships, Information Security Incident Management, Information Security aspects of Business Continuity Management, Compliance.[2]

However, 35 control objectives and 114 controls are explicitly suggested here and the explanations to those are clearly provided for effective guidance in ISO/IEC 27002:2013. If an organization applies the risk management effectively and comprehensively at the organizational level (not in silos at the functional level) using this standard, there is a good chance that the organization will be able to face the information security threats quite effectively.

NIST Special Publication 800-39 complemented by 800-53

The NIST special publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View, provides guidance on integrated organization-wide risk management.[3] Chapter Two of this special publication describes:

- The components of risk management
- The multi-tiered risk management approach
- Risk management at the organization level (Tier 1)
- Risk management at the mission/business process level (Tier 2)
- Risk management at the information system level (Tier 3)
- Risk related to trust and trustworthiness
- The effects of organizational culture on risk
- Relationships among key risk management concepts

Chapter Three describes a life cycle-based process for managing information security risks including:[3]

- A general overview of the risk management process
- How organizations establish the context for risk-based decisions
- How organizations assess risk
- How organizations respond to risk
- How organizations monitor risk over time

As you can see from the above, the risk management process is focused on three specific layers – the organization level (Tier 1), the mission/business process level (Tier 2) and the information system level (Tier 3).

The NIST special publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations, provides guidance on assignment of effective security controls during the multi-tiered risk management approach.[3]

Chapter Two describes the fundamental concepts that are associated with security control selections and specification including:

- Multi-tiered risk management
- The structure of security controls and how the controls are organized into families
- Security control baselines as starting points for the tailoring process
- The use of common controls and inheritance of security capabilities
- External environments and service providers
- Assurance and trustworthiness
- Revisions and extensions to security controls and control baselines

Chapter Three describes the process of selecting and specifying security controls for organizational information systems including:[3]

- Selecting the appropriate security control baselines
- Tailoring the baseline controls, including developing specialized overlays
- Documenting the security control selection process
- Applying the selection process to new and legacy systems

The application of SP 800-39, complemented with SP 800-53, provide a good foundation for any organization. Furthermore, other NIST special publications like SP 800-30 Rev 1 Guide for Conducting Risk Assessments give a detailed guideline on each of the steps of risk assessment.[3]

SABSA®

SABSA® is an open, generic, scalable methodology for formulating information security architecture and information assurance architecture, from The SABSA Institute. The beauty of the SABSA methodology is that it bases its information security architecture on business requirements, technology enablers required for business, and business requirements for information security.[4] As such, the usual conflict of business users being adversely impacted or not happy with information security is avoided and thus, the usual resistance for information security from the business users.

SABSA specifies a six layered architecture for information security with five vertical layers, namely the Business View or Contextual Security Architecture Layer, the Architect's View or Conceptual Security Architecture Layer, the Designer's View or Logical Security Architecture Layer, the Builder's View or Physical Security Architecture Layer, and the Tradesman's View or Component Security Architecture Layer and a horizontal layer supporting all the layers, i.e., Service Security Management Architecture Layer.[4] The SABSA layered structure is depicted for easy reference in Figure 3-4.

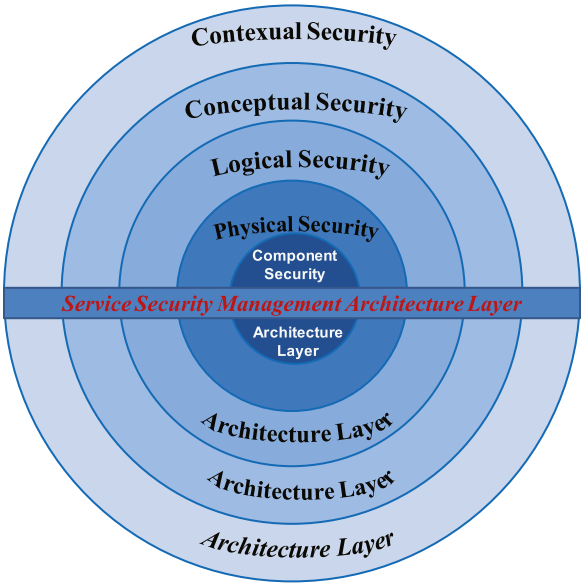

Figure 3-4. *SABSA information security architecture*

On the Contextual Security Architecture Layer, Business Users provide the business requirements that must be met by the architecture. At the Conceptual Security Architecture layer, an architect provides the overall context by which the business requirements of the organization are to be met. On the Logical Security Architecture layer, the Designers provide a systems engineering model which views the business as a system and delineates it in terms of a system of systems through various sub-systems. On the Physical Security Architecture layer, the builder provides physical security mechanisms and the servers that will be required to provide these services. On the Component Security Architecture layer, the tradesmen work on specifications provided by the builder and work with specialist products and system components which together, build what was expected by the builder. On the Service Security Management Architecture layer, the service manager deals with the system operations and service management work. Each subsequent layer builds on the output of the earlier layer, whereas the sixth layer, i.e. the Service Security Management Architecture layer, provides support to the other five layers. The security layers are described in Table 3-2.[4]

Table 3-2. *The SABSA® Information System Architecture layers*

Security Layer	Description
Business View or Contextual Security Architecture	The goals the business wants to achieve; the functional description of the same; the users, their requirements, their numbers, etc.; locational requirements and dependencies; usage patterns over time, etc. Primary considerations are: the business and its assets which need to be protected and the business needs for information security; business risks expressed in terms of business opportunities and the threats to business assets; business processes that require security; structural aspects of business security including external support structures; business geography and location-related aspects of business security; the time-related aspects of business security.
Architect's View or Conceptual Security Architecture	What needs to be protected expressed in terms of SABSA Business Attributes; the importance of protection in terms of controls and enablement objectives; how to achieve this protection through high-level technical and management security strategies, business process mapping framework; who is involved in the security management in terms of roles and responsibilities; where the architect wants the protection to be conceptualized in terms of security domains; when the protection is relevant in terms of a business time-management framework.
Designer's View or Logical Security Architecture	The business information that needs to be secured; security and risk management requirements for securing the business related information; specifying the logical security services and how they fit with each other; specifying the entities, their inter-relationships, their attributes, authorized roles and privilege profiles, etc.; specifying the security domains and inter-domain relationships; specifying the security related calendar and time-frames, etc.
Builder's View or Physical Security Architecture	Specifying the business data model and the security related data structures; specifying the rules that drive the logical decision making within the system; specifying the security mechanisms including the physical applications, middleware, servers, etc.; specifying people dependency in terms of human interface and access control systems; specifying the physical layout of the security technology infrastructure, etc.

(*continued*)

Table 3-2. (*continued*)

Security Layer	Description
Tradesman's View or Component Security Architecture	ICT components including data repositories and processors; risk management related tools; process tools and standards; personnel management tools and products; locator tools and standards; step timings and sequencing tools, etc.
Service Manager's View or Service Security Management Architecture	Service delivery management; operational risk management; process delivery management; personnel management; environment management; schedule management.

Table 3-3 summarizes the three frameworks.

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

Security is a continuous process. It involves people, policies, procedures, processes, and technology. These three categories can be considered the pillars of information security. These pillars of security and their interconnections are depicted in Figure 3-5.

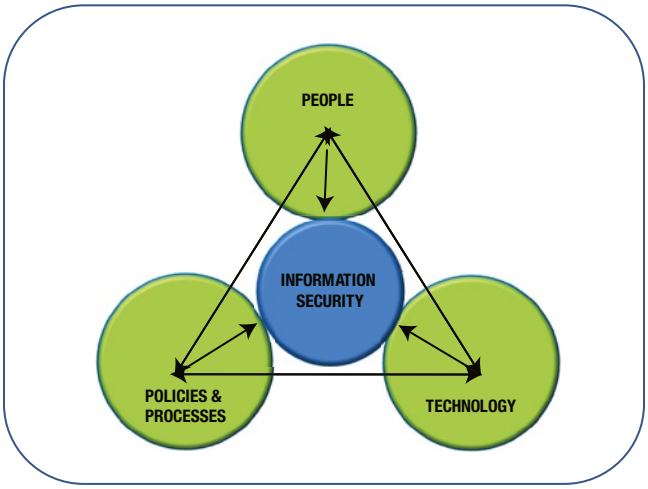

Figure 3-5. *The People, Processes, and Technology triad for information security*

As we saw in the foregoing paragraphs, people are an important, unforgettable part of information security. Effective information security involves the assignment of clear roles and responsibilities of people in any organiztion.

People

Without people there is no need for or possibility of any information security. People are the strongest pillars of the information security on the one side. But, they may sometimes tend to be the weakest pillars because of the lack of awareness or bad motives. They are easily prone to social engineering attacks or other malicious attacks. Hence, for strong information security their awareness, vigilance, and positive involvement must be increased and ensured.

Organization of Information Security

Every organization creates its structure from a functional and administrative point of view. This is very important from the perspective of the efficiency and effectiveness of work, which allows an organization to grow. However, with the widespread use of computers, the Internet, reliable connectivity, new technologies, and awareness of these new technologies among children to adults, it has become increasingly important to assign roles and responsibilities from the perspective of information security. Effective implementation of information security provides the customers, the management of the organization (including the shareholders), the employees of the organization, and all other related stakeholders the requisite assurance about an organization.

In the context of an organization, it is not enough that only the top management is concerned about information security, but it is important to involve everybody down the line, including the receptionist, the security staff, and the housekeeping staff. This requires commitment from all levels of an organization to ensure the effectiveness of implementation of information security. As it is said, "The strength of a chain is only as good as its weakest link."

With every passing day, organizations are acquiring more information processing facilities, off the shelf software, and customized software, and we know that our dependency on IT is only going to increase significantly in the coming years. Hence, it is necessary that we are proactively organized to plan and implement information security to protect ourselves, our customers, our partners, our suppliers, and other relevant stakeholders. We also need to organize ourselves to avoid, deter, prevent, detect, investigate, and overcome the issues related to information security or information security breaches.

The Need for Independence

Technology within an organization is normally headed by a Chief Technology Officer (CTO) or a Chief Information Officer (CIO). He is supported by others like IT Managers and operations staff such as system administrators, database administrators, network administrators; development staff such as programmers and support staff; and others, as relevant. Many organizations also provide information security responsibility for the same role as a CTO/CIO. It is possible in some organizations that this may not create any significant conflict of interest or issue because of the maturity of such a person, the size of the organization, or because of the maturity of others in the organization. However, it is possible in many organizations because of a conflict of interest primarily due to a lack of adequate maturity in such a person, that he may not give adequate attention to information security either because of "confirmation trap or functional fixation".[5] He may also find the need to cover up or not to publicize information security incidents in order to save himself, his personnel, or to increase the investment in information technology tools, rather than on information security related aspects. We strongly feel that there should be a clear segregation of duties between IT and information security. We strongly advise that there should be a role similar to Chief Information Security Officer (CISO) or Information Security Officer (ISO) in any organization to ensure effective independence and a non-biased view on information security. In our opinion, as the organizations and their interfaces with the external world increase in complexity, the segregation of duty in information security is also important like in any other functional areas, including finance and human resources. This segregation of duties also provides an additional view point on the same aspect.

Specific Roles and Responsibilities

Ideally, for successful implementation of the information security, it should follow a top-down approach with a clear commitment from the top, including the board of directors. If this is not the case, information security may only be seen as implemented or being implemented on paper without much success at the ground level. Even though there is no uniformity of approach as far as how various organizations have organized the information security related roles, many organizations who are serious about the implementation of information security with real intentions (not to just show the outside world or to get the certification) will have clearly assigned specific roles which handle information security in earnest.

Audit Committee or Information Security Committee at the Board Level

If we take the top-down approach, we should have at the board level, either as a part of an audit committee or as a part of a separate information security committee, a person from the board responsible for looking into information security implementation at the organization level. She should be such a person who need not be a technological expert, but who has her ears and eyes open to the external world and assimilates all issues related to information security at the global and various organizational levels. She should be a person who is actually interested in information security, and asks the tough questions on any proposal for new information processing facilities, modifications to the existing information processing facilities, new acquisitions of critical pieces of software of significant influence on the business, or of any information security aspects. These questions should not be asked just for the sake of asking them, but with all the seriousness of really understanding what the information security risks that an organization is undertaking/undergoing at any point of time or is likely to undergo in the future. She should advocate for and be the representative at the board meeting for the need for information security and convince other board members on filling the gaps related to information security.

Information Security Sponsor or Champion

The CEO or the president of the organization himself has to demonstrate commitment to information security by being the sponsor or champion of information security. This ensures that information security gets automatic buy-in in the organization when it is publicized that the CEO or the president himself is the champion of information security and he takes it very seriously. It is not enough that such a person only becomes a champion by designation or nomination, but also that he takes information security seriously and demonstrates it by his practice. It is necessary that such a role leads by example. The role of such a CEO or president as the information security champion or sponsor is primarily to:

- Promote the culture of information security in the organization
- Communicate strongly and sincerely the need for information security
- Appoint/assign other such roles so as to effectively implement information security within the organization
- Support the funding of information security projects
- Demonstrate a high commitment to information security

Chief Information Security Officer or Information Security Officer

There should be a senior person at the top management level, well empowered by the board, CEO, or the president of the organization, to head the information security cell, that is, a Chief Information Security Officer or an Information Security Officer. Ideally the role of such a person is to:

- Understand the information security risks to the entire organization, including to the business, information processing facilities, IT environment, and physical environment, both from the external and internal perspective
- Ensure that the risk assessment is carried out and the risk mitigation plans are put into effect when necessary
- Guide the entire organization on the need for information security
- Determine appropriate policies in the context of various areas of relevance to information security
- Determine and publish various procedures or work instructions to implement the policies of relevance to information security
- Educate and motivate internal and external stakeholders, including the suppliers and contractors to effectively implement information security requirements
- Analyze information security incidents and take the corrective actions as appropriate to information security related incidents
- Ensure that personnel of the organization, suppliers, contractors, and customers as necessary are educated or are made aware of the means of ensuring information security
- Coordinate with external agencies/forums to understand the prevailing or possible information security issues
- Report the status of information security in the organization to the CEO, the president, or the Board, as required

In the interest that information security is successfully implemented in the organization, the CISO/ISO has to consult with and involve other functional heads, including IT personnel, suppliers, contractors, and others. The greater the extent of involvement of various people on all levels, the greater the success of the implementation of information security in any organization. Periodic risk assessment, ongoing diligence, regular training of the staff on information security, and motivating staff and others to bring information security events to the organization's knowledge are very important in the entire list of responsibilities. He should have a good reporting mechanism of the various security events or incidents, so that they get his requisite attention and appropriate corrective actions can then be determined.

Information Security Forum

We have seen that in many organizations, there is a forum created, usually known as the Information Security Forum, consisting of the CTO, the CISO, the Business Representatives and department/functional heads to ensure that there is always an exchange of information and discussion on the implementation of different action plans related to the information security risks that the organization is facing at that point in time or is exposed to in the future. Business representatives are important constituents of this forum as they provide the business goals, how the technology needs to enable business, and business requirements of information security, thus providing the mandatory piece of information for planning and the implementation of any effective information security system. Such a forum can be both educational and action oriented. Having such a forum at the organization increases the buy-in factor for information security projects or information security related action plans in the organization and provides a better, more positive push in the direction of information security implementation. We strongly feel that such a forum needs to be created in every organization.

Information Security Specialists

The CISO/ISO should be assisted by either independent security specialists from outside or inside the organization. It is necessary that their views are heard with attention, considered adequately, and are acted upon where found relevant, applicable, and useful. If their recommendations are not implemented, the CISO/ISO should be informed. They should be encouraged to come up with their own views and bring them to the table. They should be motivated to speak of current or potential issues. With them being active on various relevant forums, they can bring up any new issues or which are being discussed as potential issues to the organizational CISO/ISO's knowledge, so that depending upon the relevance and severity of such issues, the organization can proactively decide on the actions to avoid, deter, prevent, detect, research, investigate, and eliminate. They also advise the CISO/ISO on technologies and products related to information security. Some of them can take roles like security architects, security designers, or security auditors.

Project Managers

Each project manager in the organization, whether he manages an infrastructural project, an IT project, a software development project, or any other type of project, should always look for the kind of information security risks he may be leading the organization to and take any necessary risk mitigation action that's necessary. Thinking of information security risks should be an integral part of project management from the initial planning stage and should continue to be considered throughout the life cycle and through design and development phases – until the successful completion of the project. Interestingly, this is one of the controls that was newly brought in by the recent revision of information security management systems – Requirements (ISO 27001:2013 – Control number A.6.1.5).[2] The need for this change was amplified in the Frost & Sullivan Market Survey (sponsored by (ISC)[2] and prepared by Robert Ayoub, CISSP Global Program Director) on information security, which claims that 73% of application vulnerabilities are one of the top security issues.[11]

Data Owners

Data owners should decide who needs access to which data. Restriction from or access to data may arise from an agreement with concerned customers. Data owners should regularly review access that is granted to users and check for the continued relevance of such access to ensure that the applications accessing the data, modifying the data, or deleting the data do so appropriately as per the business requirements.

Data Custodians

Data custodians are not owners of the data, but by their job roles, they are designated as the custodians of the data, such as database administrators. They have access to the entire set of data, but have to be very careful to ensure that such access is utilized only as per their role and primarily should be used to preserve the confidentiality, integrity, and availability of the data to the rightful and authorized persons. They should act on authorization requests based on the approval of the data owners. They should also exercise caution and due diligence in all their activities.

Users of the data

Users of the data have a huge onus in protecting and ensuring information security. They should be guided by their terms of access and the need for access. They should access only such data which is of relevance to them in completing their assigned roles and responsibilities. They should follow all the policies, procedures, work instructions, and guidelines to ensure that they protect information security. They should take information security seriously and be vigilant to ensure that even others do not violate these policies, procedures, work instructions, and guidelines. Some roles and important responsibilities are described in Table 3-4.

Table 3-4. *Important information security roles and responsibilities*

Role	Responsibility
Audit Committee of the Board	• An advocate of information security at the board level and convince other board members of the importance of information security • Bring sufficient focus on information security aspects in various decision making processes
Information Security Champion or Sponsor	• Promote the culture of information security within the organization • Assign/appoint appropriate roles to effectively support information security • Promote strongly and sincerely the need for information security
CISO	• Ensure proper risk assessment and determination of appropriate controls • Ensure the definition of appropriate policies, procedures, and processes • Coordinate with other agencies and forums to understand threats to information security • Report the status of information security to the management • Motivate and train employees, contractors, and suppliers on information security do's and don'ts
Information Security Forum	• Ensure collaboration across all functions/departments-including business • Ensure a focus on the execution of information security across the organization
Information Security Specialists	• Provide an unbiased and frank opinion on current or potential risks related to information security • Assist the CISO in an effective understanding and implementation of information security requirements, risks, architecture, products, and technology

(*continued*)

Table 3-4. (*continued*)

Role	Responsibility
Project Managers	• Consider information security related risks and mitigate them throughout the project life cycle
Data Owner	• Understand the characteristics and sensitivity of the data and provide the appropriate access/restrict access • On a periodical basis, review the access granted to ensure its continued appropriateness
Data Custodian	• Ensure the safety of the data and act as per the directions of the data owners
Users of the Data	• Ensure that data is used only for the purposes for which it is intended • Follow all the policies, procedures, and processes diligently to ensure the security of information assets

Authority for Information Security

Empowerment or authority should be vested as appropriate in each of the above roles in order for them to be effective. Definitely the CISO or the ISO should have the authority to stop any activity which is going to lead the organization into severe information security lapses or issues. Everyone in the information security forum should have the authority to demand information security primarily to protect the business, its customers, and its partners. Information security specialists in the organization should have the authority to demand that they be heard. Such an authority should be vested in such roles by the board, CEO, or the president of the organization and make it clear across the organization.

Policies, Procedures, and Processes

Information security is incomplete without clearly defined policies which guide employees, contractors, and suppliers. Policies provide guidance to everyone and depict the commitment of management to them. The following are some of the policies that are important to most of the organizations, as per ISO/IEC 27001:2013:[2]

- 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
- Protection from Malware Policy
- Management of Technical Vulnerabilities Policy

- Information Transfer Policy
- Communications Security Policy
- Cryptographic Controls Policy
- Policy on Supplier Relationships

Some of the other standards like Information technology – Service management – Part 1: Service management system requirements (ISO/IEC 20000-1:2011) call for more policies.

Procedures and processes describe how the intent of the policies is to be implemented. They detail step-by-step instructions on how to carry on the work so that the intentions of these policies are adhered to. Training the employees, contractors, and suppliers on the relevant policies, procedures, and processes is a must in order to ensure that these are understood. With the ever-evolving business environment, challenging risks, and changing technologies policies need to be reviewed and kept current. Thus, the training process should be ongoing and continual.

Technology

Technology is another important pillar. There are many good and competing technologies available to protect information security. All these technologies need to be explored within the entire context of the organization to ensure they seamlessly integrate with the overall fulfilment of both business and information security requirements. Technology should fulfil the requirement of information security architecture. Business and its risks and opportunities should be the main focus and technology should be an enabler rather than the end to meet the same.

Some of the important technologies available are auto monitoring and alerting systems, logging systems, detecting systems, preventive systems, and recovery systems. Examples are firewalls, IDS/IPS, and anti-virus software.

Information Security Concepts

What constitutes information security? What are we protecting through information security? This requires sufficient consideration if the field of information security is to be better understood. The following discussion sheds light on the important aspects or constituents of information security.

CIA Triad

The compromise of information security is one of the biggest issues faced by the IT and IT enabled industry, which is almost every industry these days. Some of the scenarios of the possible compromise of information security are depicted in Figure 3-6. Figure 3-7 depicts one of the important models of information security popularly known as CIA Triad.

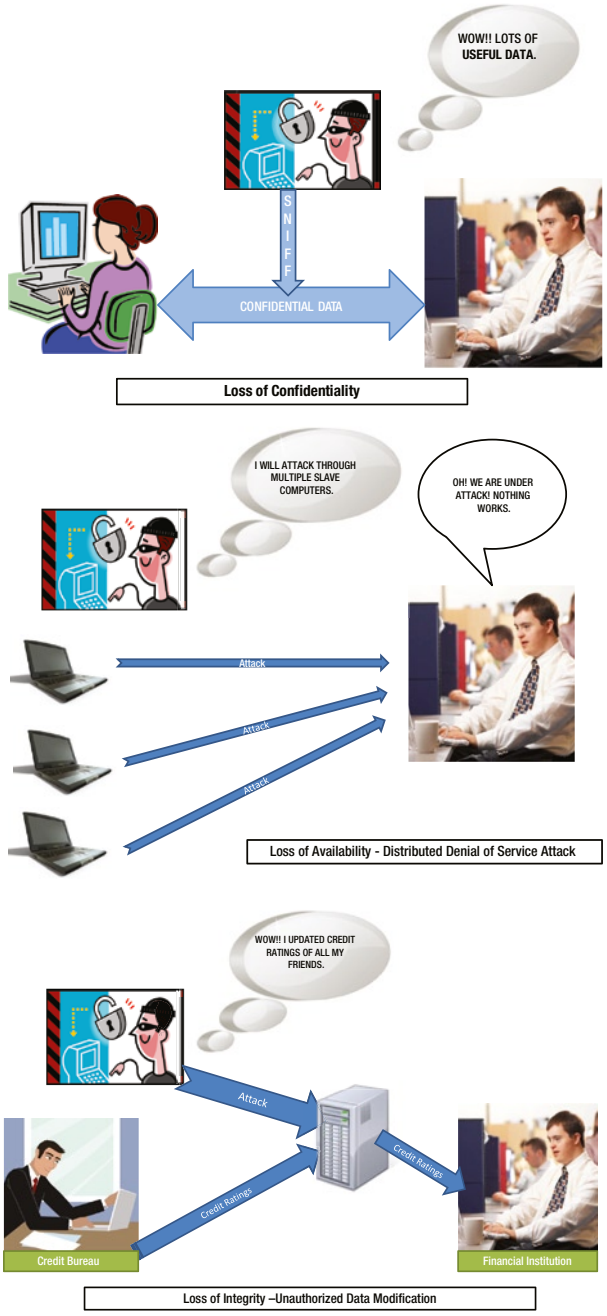

Figure 3-6. *The compromise of information security*

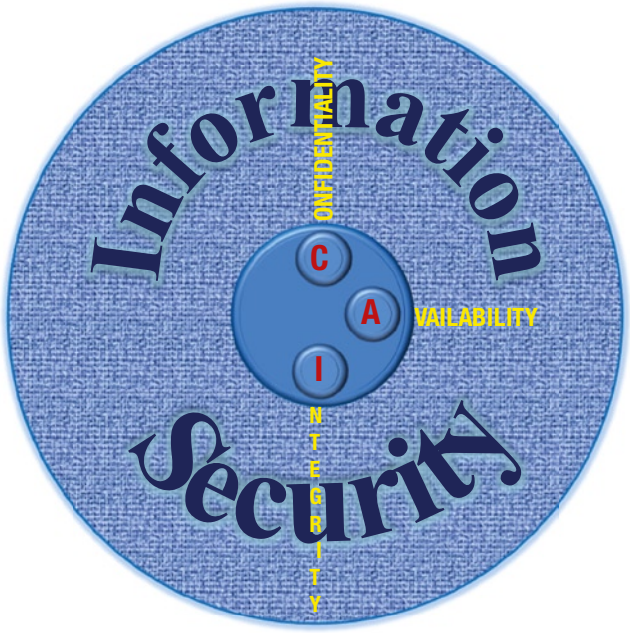

Figure 3-7. *CIA triad*

■ **Note** As mentioned in the introduction to this chapter, the CIA triad is one of the most important models of information security which specifies the important properties or characteristics of information assets, without which, an understanding of information security is not possible. However, the importance of the CIA triad has increased in recent years because of the way we input, transfer, or store the information. Mainly, "confidentiality" has taken a bigger beating compared to the other properties.

Traditional definitions/views on "confidentiality", "integrity," and "availability" came from the National Institute of Standards and Technology (NIST)/U.S.Code and are the most referred and used ones. However, if you look at the definitions from various organizations or standards organizations active in the field of information security, you will be quick to realize that each definition varies from the other and hence, these definitions may not be all pervasive and comprehensive. Some of the popular definitions are reviewed in the following sections.

Confidentiality

Some information is secret, sensitive, or needs to be restricted as a disclosure to unintended sources can create such things as the compromise of a nation's security or strategic installations, the loss of business opportunities, a first mover advantage, intellectual property rights, and privacy. Such information is considered in general terms as "confidential" and needs to be protected zealously by appropriate authorization or restrictions. Consider the following scenarios to fully understand:

- You have decided on a business strategy to counter a competitor and it is leaked to others accidentally or by an aggrieved senior management person who just left the organization.
- You have innovated a new technological idea and want to patent it. But, before you patent it, the same idea is copied by someone and further passed on to someone else and is patented by them instead.
- The patient information and medical records of the patients you have stored have been stolen and made public.
- You find that one of the administrative passwords is compromised and significant data of confidential nature has been stolen.

Chapter 44, Title 35, Subchapter III, and Section 3542 of the U.S.C. defines "confidentiality" as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [NIST SP 800-100]".[6]

Information security management systems – overview and vocabulary (ISO/IEC 27000:2014) defines "confidentiality" as "property that information is not made available or disclosed to unauthorized individuals, entities, or processes".[7]

Integrity

Information is useful and reliable only if it is accurate and not modified against the intentions wanted of the originator. "Integrity" needs to be protected appropriately by means such as appropriate authentication, routing protocols, appropriate configuration of systems, and application security. Consider the following scenarios to understand:

- You have received a letter purported to be from a customer company and they have sought some important information to be divulged to one of their suppliers. You find something fishy in the letter and upon investigation, you find that the letter was fake and originated by a supplier company and not by the customer company.
- You divulged critical, confidential information about the strategy of your competitor company, purported to be leaked by one of their employees, but you find that it was conveyed to you in a misleading way in order for you to make the wrong decision.
- You were given the correct information, but only a portion of it, whereas the other portion of the information which was crucial if you would have been told would have given you an entirely different perspective on the matter.

Chapter 44, Title 35, Subchapter III, and Section 3542 of the U.S.C. defines "integrity" as "guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity [NIST SP 800-100]".[6]

Information security management systems – overview and vocabulary (ISO/IEC 27000:2014) defines "integrity" as "property of protecting the accuracy and completeness of assets".[7]

Availability

Information today is stored in systems, databases, storage units, or, most recently, on the Cloud. In today's fast-paced world where opportunities can be lost fast and the speed of decision making is important, the availability of crucial information at all times has become necessary. Consider the following scenarios to understand this concept:

- You are required to send an important note to your customer and you find that your e-mail system or Internet is not responding.
- You are required to carry out certain work and your reference documents are in a particular database and the particular database is down for technical reasons.
- You are required to initiate an important request through one of your applications and you find that the application is not responding.

Chapter 44, Title 35, Subchapter III, of Section 3542 of the U.S.C. defines "availability" as "ensuring timely and reliable access to and the use of information. [NIST SP 800-100]".[6]

Information security management systems – overview and vocabulary (ISO/IEC 27000:2014) defines "availability" as "property of being accessible and usable upon demand by an authorized entity".[7]

For information security to be complete and the organizations or individuals to be protected, it is necessary that all three properties or aspects are to be ensured. Emphasizing only one at the cost of others may lead to the reduced efficiency and effectiveness of any organization.

Parkerian Hexad

Donn B. Parker, one of the information security specialists of repute, brought out some alternate perspectives of the properties of information security. In addition to the three properties specified through the CIA triad, he brought out three more descriptors or properties, namely, possession, authenticity, and utility, thus forming a hexad known as the Parkerian Hexad. The Parkerian Hexad also groups confidentiality and possession, integrity and authenticity, availability and utility, pairs together as these are related.[8]

The definitions provided by the Parkerian Hexad for the six properties or descriptors are as follows:[8]

- "Confidentiality" is defined as the "quality or state of being private or secret; known only to a limited few."
- "Possession or Control" is defined as "a state of having in or taking into one's control or holding at one's disposal; actual physical control of property by one who holds for himself, as distinguished from custody; something owned or controlled."
- "Integrity" is defined as "unimpaired or unmarred condition; soundness; entire correspondence with an original condition; the quality or state of being complete or undivided; material wholeness."
- "Authenticity" is defined as "authoritative, valid, true, real, genuine, or worthy of acceptance or belief by reason of conformity to fact and reality."
- "Availability" is defined as "capable of use for the accomplishment of a purpose, immediately usable, accessible, may be obtained."
- "Utility" is defined as "useful, fitness for some purpose."

The Parkerian Hexad describes "confidentiality" as a little different from the traditional definition of "confidentiality" that is provided by U.S.Code/NIST. This hexad considers "possession" as an important element which may impact confidentiality. The "possession" of confidential information can sometimes lead to such threats

like blackmail, extortion, sabotage, or destruction. Similarly, proprietary and personal information considered by traditional definition to be confidential may in fact be confidential or not confidential, depending upon the nature of the information or timing of the information divulgence.[8]

The Parkerian Hexad describes "integrity" as a little different from the traditional definition of "integrity" that is provided by U.S.Code/NIST. This hexad doesn't consider "authenticity" as a part of "integrity" and as a different property, which has to do with the validity or genuineness of the information than the unimpaired condition of the information. Again here, "non-repudiation" is considered a different aspect than "integrity" and as related to "authenticity" as it refers to validity or genuineness of the information.[8]

Parkerian hexad considers "availability" along with "utility" as information even if available is of use only if it is usable or has utility. It differs from the traditional definition in that "availability" has nothing to do with "reliable access".[8]

As seen above, the Parkerian Hexad gives a different perspective of the characteristics or properties of information security.

A simple view of the above properties is represented in Figure 3-8.

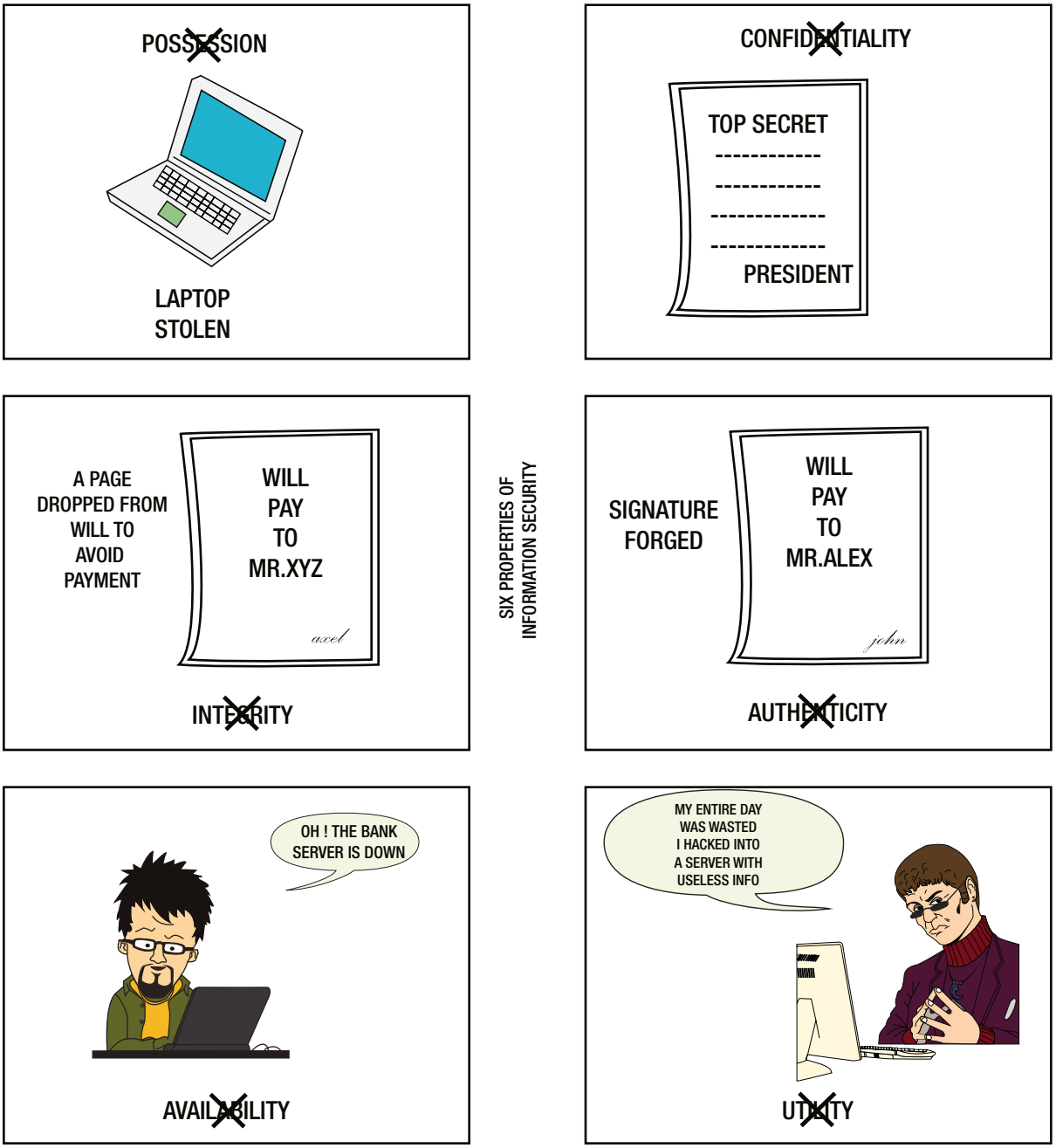

Figure 3-8. *Six properties of information security with simple examples*

Implementation of Information Security

It is not easy to implement information security. All the pillars of information security have to be given adequate thought. Proper scoping has to be done for the efforts and proper planning has to be done involving all the stakeholders. Planning has to be backed by strong execution of the same and overcoming the barriers as execution is carried out. Focus on ensuring the success of implementation is necessary with all the relevant people assigned and involved appropriately.

Figure 3-9 gives the typical information security implementation cycle. Depending upon the context of the organization there may be different models used for implementation.

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

An effective approach to the implementation of information security is the key to its success. Organizations at different stages of their existence may approach the implementation in different ways. An organization already in existence usually drives its journey on the path to information security primarily through the initiation of risk assessment. Hence, various standards and frameworks highlight the risk assessment aspect as the important step in the overall context of implementation of information security. However, a new organization may initiate its journey on the path to information security through the determination of its business requirements, determination of infrastructural and technological requirements to facilitate/enable business, and through the determination of business requirements for information security like the one suggested by SABSA methodology.

Risk Assessment

There are various risk management methodologies available for ensuring effective risk assessment. Some of them are: Risk Management – Principles and guidelines (ISO/IEC 31000:2009); Operationally Critical Threat, Asset and Vulnerability Evaluation [SM] (OCTAVE®) from Software Engineering Institute, CMU, Pittsburgh;[9] risk assessment methodology specified by NIST (SP 30, 39 & 53); Risk IT framework by Information Systems Audit and Control Association, US;[10] and FMEA. An organization can use any methodology but the risk assessment as a process has to be carried out methodically and effectively to derive the required benefits. An understanding of the risks in the context of the entire organization, keeping in mind the vulnerabilities and threats to information assets even from the outside world, understanding the current controls that are in place and quantification of the risk to understand

risk exposure normally drives the risk response including the risk mitigations to be carried out. Risk mitigations are determined based on the effective controls already implemented by other organizations, suggested by other agencies, by implementation of tools, through policies and processes, through other additional controls as required including awareness and training of the employees, contractors and suppliers, or through deterrents like legal agreements. Employees normally include temporary workers too.

Planning and Architecture

In an existing organization, planning may commence with the commencement of planning for effective risk assessment involving all the stakeholders as relevant. In a new organization, the planning may be carried out to effectively approach achievement of information security using relevant steps as suggested by appropriate frameworks or methodologies. Plans also identify the owners for various activities, roles, and responsibilities for the effective execution of these plans. The schedules used also clearly depicts the timelines, keeping in mind various dependencies and constraints. The steps planned depend upon the methodology or framework used. Planning needs to be carried out for an integrated, methodical, and well-coordinated approach, leading to effective information security infrastructure or architecture rather than an ad-hoc approach that can create side effects or make the implementation ineffective. Effective information security infrastructure or architecture provides ease of use and generates confidence to all the stakeholders including business users.

In an existing organization, risk assessment provides the input for the planning. The implementation of additional controls determined to mitigate are planned through the risk treatment plans. These actions are clearly assigned to the appropriate owners with clearly identified timelines. Well-implemented risk treatment plans ensure that the organization is well protected.

Gap Analysis

Things change: the business may change, the technology changes, the people change. Changes are the only constant in today's world. Also, the vulnerabilities until now unknown will have been exposed to the world or reported. Hence, we have to ensure that our protection systems continue to work even under these constant changes. In order to ensure this, a periodical gap analysis needs to be carried out which sometimes throw up significant surprises. This 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. This may be done through periodical risk re-assessments leading to additional controls to be implemented through new risk treatment plans.

Integration and Deployment

As discussed earlier, any implementation done in silos rather than organization-wide does not provide adequate protection. Instead, it can create an inconvenience in the usage and also expose us to more threats. Hence, an integrated view at all times in the totality of the business and the organization is required. Also, an effective deployment of all intended policies, procedures, and processes, along with the intended implementation of information security architecture and its various layers is required. All the efforts related to information security need to be thought of in an integrated manner by involving all the relevant stakeholders and need to be implemented based on their dependencies. Incomplete implementation or inadequate attention to any one of the layers may defeat the controls built in other layers. For example, there is no use in implementing a tool for the analysis of the alerts unless the persons who are required to analyze them are trained on the same. Similarly, implementation of new policies and procedures will be useless unless the persons who should understand them and follow them are not aware of them or are not trained on using them. The implementation of new tools is of no use unless the internal people know how to configure and use them effectively. 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. All these steps need to definitely be a part of the planning we talked about earlier in the chapter.

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. Similarly, not carrying out certain activities which are essential as per the policies and procedures, can defeat the very purpose of information security. Hence, operations should be tightly controlled for effective information security. For example, backups were not taken because the system administrators were busy on another activity. This defeats the protection provided through backups. The installation of a patch without taking sufficient precautions can bring down the system itself. Not carrying out the maintenance of UPS can bring down the UPS leading to an abrupt shutdown of the systems leading to system or data corruption. All operations should be guided by appropriate processes (standard operating procedures) and carried out as per the plans. A non-maintained earth pit can be a significant issue. Not checking the backup media through periodical restoration may lead to the tape being not readable or restorable when required.

Monitoring

Monitoring is an integral part of any activity whether it is business related or information security-related activity. Any organization needs to keep monitoring the threats to it so that it can react to the threats effectively and on time. This activity is time-consuming. 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. For example, 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. In the field of information security, in order to understand the causes of the breaches and incidents, sometimes the forensic analysis (where the causes may not be obvious or straight forward) may have to be carried out. This will enable us to understand the causes clearly and put in place our defensive mechanisms so that such incidents can be avoided or reduced.

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. Sometimes, organizations may be made to shell out huge penalties for non-compliance or negligence. Furthermore, there are a lot of laws enacted to prevent the misuse of information technology and those need to be adhered to. These 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 to understand the non-compliance issues and plug them out before they become severe.

Another thing to consider here is the compliance check on various policies, procedures, or processes implemented by the organizations. We all know that most of the time, these policies or processes are written wonderfully, but people who are trained on them over a period of time, these can be forgotten. Sometimes, the context changes, but these policies and processes are not modified. New employees join the organization but they are not trained on these policies and processes. Normally, in almost all of the organizations, most of the employees are always on either fighting one or other types of business fires, working on or solving one or another crucial burning issue. Consequently, the requisite attention and focus on effective implementation of these policies and processes takes a back seat or gets into a low priority mode. Hence, it is strongly suggested that every organization should have strong periodic internal audits coupled with external audits by independent experts occasionally. The non-conformances identified and the suggestions made in these audits should be placed before the management and necessary actions have to be determined and implemented across the organization. Management should provide necessary focus on these so that even if the organization wades off a little, it is again brought back to the right path.

Crisis Management

The Crisis Management Plan, Business Continuity Plan, or Disaster Recovery Plan are interchangeably used to denote a single entity, even though there are subtle differences between them. For the purpose of discussion here, let us consider them as 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 cannot sit idle. They need to respond effectively and also restore their business back to normalcy after such attacks. Towards this purpose, a well-planned business continuity and crisis management plan should be put in place by every organization. Disaster recovery and business continuity should become an integral part of the planning process of every organization. Ideally, every organization should carry out the business impact analysis to identify the critical businesses for which continuity is essential and also the tolerance time frame up to which the organization can wait before the business need to be commenced. A business continuity plan should be put in place clearly identifying the roles and responsibilities of all the concerned stakeholders. All the stakeholders need to be trained and the business continuity plan should be tested to check that it works as required when actually it has to be put into action. Crisis declaration is an important step. As every event or incident is not a crisis, a senior person should be empowered to identify a crisis when it arises, as he has the maturity and knowledge to declare a situation a crisis.

Principles of Information Security

If you look closely, you will find that there is going to be a close relationship between what we discussed so far in this chapter and what we are going to discuss here. The principles of information security were established as far back as 1996 by the National Institute of Standards and Technology of United States of America through Special Publication 800-14: "Generally Accepted Principles and Practices for Securing Information Technology Systems." We feel that these fundamental expectations are valid and relevant even in today's context.[12]

While there are many approaches that may be used to ensure information security, there are some minimum expectations which need to be met invariably by all the current systems, irrespective of their size. These eight fundamental principles of information security are the ones which we are going to discuss in brief in the following paragraphs.[12]

- 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.

- 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.

- 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.

- 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.

- 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. In our discussions, earlier in this chapter, we have elaborated on the whys and hows of clear demarcation for information security, roles, responsibilities, and authorities will ensure successful compliance towards information security. Negligence cannot be excused in the field of information security as organizations can be severely affected with reputation loss, business loss, penalties, etc. Accountability is brought in clearly and effectively through clarity on roles, responsibilities, and authorities.

- 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.

- 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.

- 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.

The aforementioned fundamental principles of information security are further substantiated through additional principles for engineering effective information security through NIST's special publication 800-27 Revision A: "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)."

Chapter Summary

- In this chapter, we attempted to lay a strong foundation for the next few chapters. We explored four important layers of information security, namely Physical Security (which includes Hardware Security), Network Security (which includes Communications Security), Software Security (which includes Operating System Security, Applications Security and Security of Utilities/Tools), and Human Security (which is people) related. We saw how each of these layers contribute to overall information security at any organization. We also saw how the policies, procedures, and processes contribute to the overall scheme of information security. Through a context diagram, we also depicted various important controls of each of these layers.
- We explored various security threats and categorized them into external threats and internal threats based on the origin of these threats. Then we identified some of the important external and internal threats under each of the layers, including Physical Security, Network Security, Software Security, and Human Security.
- We also explored the generic multi-layered approach to information security architecture which can be used by any organization and we looked at important components of each of these layers. We also looked at additional aspects covered by "defense-of-depth" and how it can help an organization to respond to information security breaches or incidents. We touched upon some of the important frameworks/architectural models of information security like ISO/IEC 27001:2013 complemented by ISO/IEC 27002:2013, NIST SP-39 and SP-53 and SABSA. We then explored the above frameworks/architectural models in detail and how these lead to a secure information security architecture for any organization. We also looked at the advantages and disadvantages of each of these.
- We examined the three important pillars of security: People, Policies, Procedures and Processes, and Technology. We explored how the organization has to equip itself for effective implementation of information security, the importance of independence of information security personnel, and what the typical information security roles and responsibilities are. We also stressed the need for clearly specifying the authorities related to information security. We then detailed how policies, processes, and technology effectively contribute to and support people in implementing information security.
- We discussed the CIA triad (which was the traditionally accepted model of information security) and the Parkerian Hexad which extended upon the CIA triad. We explored some of the important definitions of confidentiality, integrity and availability from the U.S.Code/NIST and other standards/forums. We went through the fact that various definitions are in variant with each other. We also looked at the variances between the definitions from NIST and those from the Parkerian Hexad. We also looked at some of the examples of each properties of information security as per CIA and as per the Parkerian Hexad.
- We suggested one approach for effectively implementing information security in any organization, that is, both a new organization and an existing organization. We elaborated upon the need for risk assessment and the various frameworks for risk assessment, importance of appropriate planning, and the need for having robust information security architecture, periodical gap analysis, and the need for execution discipline in operations, the importance of regular monitoring, the importance of legal compliance and periodic audits, and crisis management.