Unit 1 Introduction to Information Security

Structure

Introduction to Information Security

Information and information systems need to be controlled. A key aspect of control is that an information system should be secure. This is achieved through security controls. What are these?

1.1 Definition of Information Security

The most widely accepted definition of Information System Security is given as:

"the practice of ensuring information is only read, heard, changed, broadcast and otherwise used by people who have the right to do so" (Source: UK Online for Business)

Information systems need to be secure if they are to be reliable. Since many businesses are critically reliant on their information systems for key business processes (e.g. webs ites, production scheduling, transaction processing), security can be seen to be a very important area for management to get right.

1.2 Potential Risks to Information System

Data and information in any information system is at risk from:

Human error: e.g. entering incorrect transactions; failing to spot and correct errors; processing the wrong information; accidentally deleting data

Technical errors: e.g. hardware that fails or software that crashes during transaction processing

Accidents and disasters: e.g. floods, fire

Fraud - deliberate attempts to corrupt or amend previously legitimate data and information

Commercial espionage: e.g. competitors deliberately gaining access to commercially-sensitive data (e.g. customer details; pricing and profit margin data, designs)

Malicious damage: where an employee or other person deliberately sets out to destroy or damage data and systems (e.g. hackers, creators of viruses)

1.3 Making Information System more Secure

There is no such thing as failsafe security for information systems. When designing security controls, a business needs to address the following factors;

Prevention: What can be done to prevent security accidents, errors and breaches? Physical security controls are a key part of prevention techniques, as are controls designing to ensure the integrity of data

Detection: Spotting when things have gone wrong is crucial; detection needs to be done as soon as possible - particularly if the information is commercially sensitive. Detection controls are often combined with prevention controls (e.g. a log of all attempts to achieve unauthorized access to a network).

Deterrence: deterrence controls are about discouraging potential security breaches.

Data recovery: If something goes wrong (e.g. data is corrupted or hardware breaks down) it is important to be able to recover lost data and information.

1.4 Business benefits of good information security

Managing information security is often viewed as a headache by management. It is often perceived as adding costs to a business by focusing on "negatives" - i.e what might go wrong.

However, there are many potential business benefits from getting information system security right: for example:

– If systems are more up-to-date and secure - they are also more likely to be accurate and efficient
– Security can be used to "differentiate" a business – it helps build confidence with customers and suppliers
– Better information systems can increase the capacity of a business. For example, adding secure online ordering to a web site can boost sales enabling customers to buy 24 hours a day, 7 days a week
– By managing risk more effectively – a business can cut down on losses and potential legal liabilities

1.5 Sources of Data & Information

Data and information come from many sources - both internal (inside the business) and external. This revision note summarizes the main sources: Business data and information comes from multiple sources. The challenge for a business is to capture and use information that is relevant and reliable. The main sources are:

1.5.1 Internal Information

Accounting records are a prime source of internal information. They detail the transactions of the business in the past - which may be used as the basis for planning for the future (e.g. preparing a financial budget or forecast). The accounting records are primarily used to record what happens to the financial resources of a business. For example, how cash is

obtained and spent; what assets are acquired; what profits or losses are made on the activities of the business.

However, accounting records can provide much more than financial information. For example, details of the products manufactured and delivered from a factory can provide useful information about whether quality standards are being met. Data analysed from customer sales invoices provides a profile of what and to whom products are being sold.

A lot of internal information is connected to accounting systems - but is not directly part of them. for example:

- Records of the people employed by the business (personal details; what they get paid; skills and experience; training records)
- Data on the costs associated with business processes (e.g. costings for contracts entered into by the business)
- Data from the production department (e.g. number of machines; capacity; repair record)
- Data from activities in direct contact with the customer (e.g. analysis of calls received and missed in a call centre)

A lot of internal information is also provided informally. For example, regular meetings of staff and management will result in the communication of relevant information.

1.5.2 External Information

As the term implies, this is information that is obtained from outside the business. There are several categories of external information:

Information relating to way a business should undertake its activities

E.g. businesses need to keep records so that they can collect taxes on behalf of the government. So a business needs to obtain regular information about the taxation system (e.g. PAYE, VAT, Corporation Tax) and what actions it needs to take. Increasingly this kind of information (and the return

forms a business needs to send) is provided in digital format. Similarly, a business needs to be aware of key legal areas (e.g. environmental legislation; health & safety regulation; employment law). There is a whole publishing industry devoted to selling this kind of information to businesses.

Information about the markets in which a business operates

This kind of external information is critically important to a business. It is often referred to as "market" or "competitive intelligence". Most of the external information that a business needs can be obtained from marketing research. Marketing research can help a business do one or more of the following:

1. **Gain a more detailed understanding of consumers' needs** – marketing research can help firms to discover consumers' opinions on a huge range of issues, e.g., views on products' prices, packaging, recent advertising campaigns
2. **Reduce the risk of product/business failure** – there is no guarantee that any new idea will be a commercial success, but accurate and up-to-date information on the market can help a business make informed decisions, hopefully leading to products that consumers want in sufficient numbers to achieve commercial success.
3. **Forecast future trends** – marketing research can not only provide information regarding the current state of the market but it can also be used to anticipate customer needs future customer needs. Firms can then make the necessary adjustments to their product portfolios and levels of output in order to remain successful.

The information for marketing research tends to come from three main sources:

Internal Company Information – e.g. sales, orders, customer profiles, stocks, customer service reports

Marketing intelligence – this is a catch-all term to include all the everyday information about developments in the market that helps a business prepare and adjust its marketing plans. It can be obtained from many sources, including suppliers, customers and distributors. It is also possible to buy intelligence information from outside suppliers (e.g. Mintel, Dun and Bradstreet) who will produce commercial intelligence reports that can be sold profitably to any interested organisation.

Market Research – existing data from internal sources may not provide sufficient detail. Similarly, published reports from market intelligence organisations cannot always be relied upon to provide the up-to-date, relevant information required. In these circumstances, a business may need to commission specific studies in order to acquire the data required to support their marketing strategy.

1.6 Methods of Data Storage

Data storage is the holding of data in an **electromagnetic form** for **access** by a **computer processor**. There are two main kinds of storage: Primary storage is data that is held in in random access memory (RAM) and other memory devices that are built into computers. Secondary storage is data that is stored on external storage devices such as hard disks, tapes, CD's. The points below summarizes the main methods of data storage

1.6.1 Hard disks

Often called a disk drive, hard drive or hard disk drive, this method of data storage stores and provides relatively quick access to large amounts of data. The information is stored on electromagnetically charged surfaces called 'platters'.

1.6.2 Floppy disks

A floppy disk is a type of magnetic disk memory which consists of a flexible disk with a magnetic coating. Almost all floppy disks for personal computers now have a capacity of 1.44 megabytes. Floppy disks are readily portable, and are very popular for transferring software from one PC to another. They are, however, very slow compared to hard disks and lack storage capacity. Increasingly, therefore, computer manufacturers are not including floppy disk drives in the products as a built-in storage option.

1.6.3 Tape storage

Tape is used as an **external storage medium**. It consists of a loop of flexible celluloid-like material that can store data in the form of electromagnetic charges. A tape drive is the device that positions, writes from, and reads to the tape. A tape cartridge is a protectively-encased tape that is portable.

1.6.4 Optical disks

An optical disc is a storage medium that can be written to and read using a low-powered laser beam. A laser reads these dots, and the data is converted to an electrical signal, finally converted into the original data.

1.6.5 CD-R

Compact Disc-Recordable ("CD-R") discs have become a universal data storage medium worldwide. CD-Rs are becoming increasingly popular for music recording and for file storage or transfer between personal conmputers. CDR discs are **write-once media**. This means that - once used - they cannot be erased or re-recorded upon. CD-R discs can be played back in any audio CD player or CD-ROM drive, as well as many DVD players and drives.

1.6.6 CD-RW

Compact Disc-Rewritable (CD-RW) disks are rewritable and can be erased and re-recorded upon over and over again. CD-RW discs can only be used on CD players, CD-ROM drives, and DVD players and drives that are CD-RW playback-compatible.

1.6.7 DVD

A DVD (Digital Versatile Disc or Digital Video Disc) is a high density optical disc with large capacity for storage of data, pictures and sound. The capacity capacity is 4.7 GB for single sided, singe layer DVD disc - which is approximately 7 times larger than that of a compact disc.

1.7 Information Security Architecture

There are many elements in a security strategy. To ensure orderliness and integration among them, a framework or architecture is needed. A comprehensive security strategy comprises a suite of inter-related safeguards structured in a hierarchical fashion, as follows, and as depicted in Figure 1:

- underlying all other components is **Infrastructure Security**, which provides protections for both technical components and organisational processes;
- at the mid-level are **Threat Management** and **Vulnerability Management**, which provide safeguards relating to, respectively, the occurrences that can cause harm, and the features of the information system that can be affected; and
- at the uppermost level, **Application-Specific Security** safeguards are needed, which address aspects particular to the context.

It is important to apply the longstanding military principle of **'defense-in-depth'**. This asserts that security architecture has to be devised such that any threatening event must break through successive layers of safeguards before it causes harm. A more recent expression of the principle is that there must be many onion-layers that have to be peeled back before serious damage is suffered.

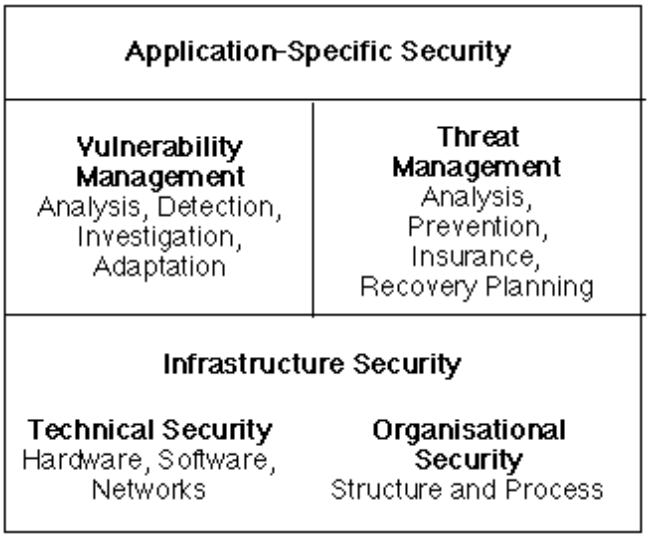

Figure 1: Information Security Architecture

1.8 The Information Security Process

The process whereby information security is assured comprises a series of phases, expressed below and depicted in Figure - 2..

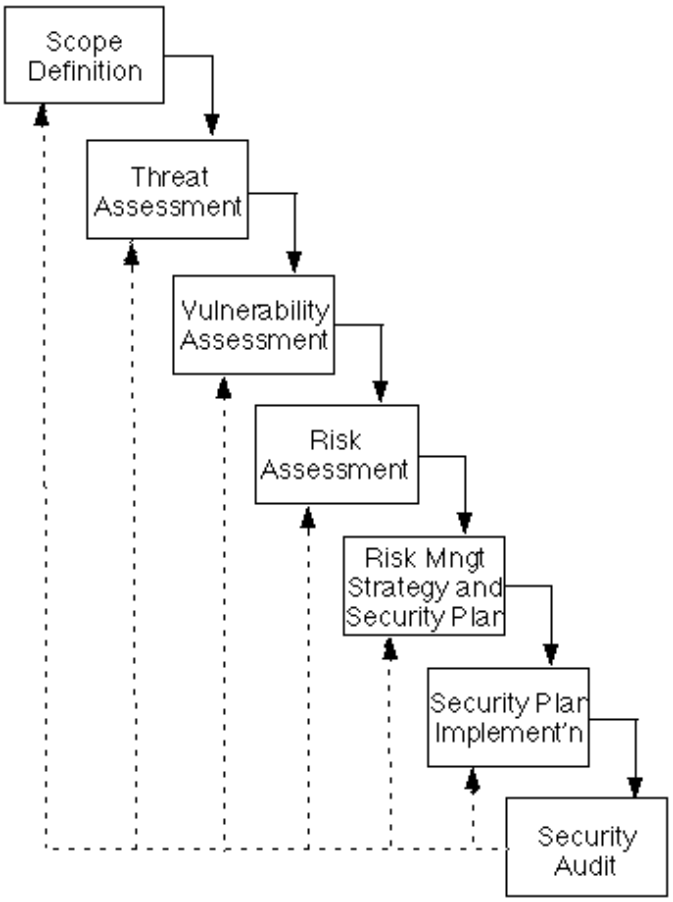

Figure 2: The Information Security Process

1.8.1 Scope Definition

A Security Strategy and Plan needs to be sculpted to the context. The first step in the process is the definition of its scope, with reference to the following:

- the set of **stakeholders**
- the **proxies** that represent those stakeholders;
- the **interests** of those stakeholders;

- the degree of importance of security in the organisation's **business strategy**, e.g. in relation to business continuity, and the accessibility and/or secrecy of various categories of data;
- the degree of importance of **public visibility of assurance** of the system's security; and
- **legal requirements** to which the organisation and its stakeholders are subject, including contracts with customers and other parties, data protection and privacy statutes, intellectual property laws, occupational health and safety, the laws of evidence, and common law obligations such as the duty of confidence, and the duty of care inherent in the tort of negligence.

It is highly desirable that the scope definition be formalised, and that relevant executives be exposed to it, and commit to it. It then sets the framework within which the subsequent phases unfold.

1.8.2 Threat Assessment

A **stocktake** needs to be undertaken of the information and processes involved, their sensitivity from the perspectives of the various stakeholders, and their attractiveness to other parties. This needs to be followed by analysis of the nature, source and situation of threats. The **nature of threats** are of a variety of kinds, including access to data by unauthorised persons, disclosure of it to others, its alteration, and its destruction. The **sources of the threats** include several categories of entities:

- a person who has authorisation to access the data, but for a purpose different from that for which they use it;
- an intruder, who has no authorisation to access the data, including:
  - an interceptor of data during a transmission; and
  - a 'cracker' who gains access to data within storage; and
- an unauthorised recipient of data from an intruder.

The **situations of the threats** include several categories of locations:

- within **manual processes, content and data storage**;
- within the **physical premises** housing facilities connected with the system; and
- within **the organisation's computing and communications facilities**, including:
  - **data storage**, including:
    - permanent storage, such as hard disk, including high-level cache;
    - transient storage, such as RAM, including low-level cache and video RAM;
    - archival storage;
  - **software** that:
    - receives data;
    - stores data (e.g. a file-handler or database manager);
    - renders data (e.g. a viewer or player);
    - despatches data; and
    - enables access to the data, in any of the above storage media (e.g. disk utilities and screen-scrapers); and
  - **transmission**, including via:
    - discrete media (e.g. diskettes, CD-ROMs); and
    - electronic transmission over local area and wide area networks;
- within **other people's computing and communications facilities**, e.g.:
  - a workstation on a trusted network that is cracked by an intruder;
  - a powerful computer that is cracked, and that is used to crack one or more passwords on the organisation's computers;
  - one or more weakly protected machines that are cracked and then used to launch denial of service (DOS) or distributed denial of service (DDOS) attacks against the organisation's servers or networks;

- within **supporting infrastructure**, including electrical supplies, air-conditioning, and fire protection systems.

1.8.3 Vulnerability Assessment

The existence of a threat does not necessarily mean that harm will arise. For example, it is not enough for there to be lightning in the vicinity. The lightning has to actually strike something that is relevant to the system. Further, there has to be some susceptibility within the system, such that the lightning strike can actually cause harm. The purpose of the Vulnerability Assessment is to identify all such susceptibilities to the identified threats, and the nature of the harm that could arise from them.

It is common for vulnerabilities to be countered by safeguards. For example, safeguards against lightning strikes on a facility include lightning rods on the building in which it is housed. Safeguards may also exist against threatening events occurring in situations remote to the system in question. For example, a lightning strike on a nearby electricity substation may result in a power surge, or a power outage in the local facility. This may be safeguarded against by means of a surge protector and an Uninterruptable Power Supply (UPS).

Every safeguard creates a further round of vulnerabilities, including susceptibilities to threats that may not have been previously considered. For example, a UPS may fail because the batteries have gone flat and not been subjected to regular inspections, or because its operation is in fact dependent on the mains supply not failing too quickly, and has never been tested in such a way that that susceptibility has become evident.

1.8.4 Risk Assessment

The term 'risk' is used in many different senses (including as a synonym for what was called above 'threat', and 'harm', and even 'vulnerability'!). But

when security specialists use the word 'risk', they have a very specific meaning for it: a measure of the likelihood of harm arising from a threat.

Risk assessment builds on the preceding analyses of threats and vulnerabilities, by considering the likelihood of threatening events occurring and impinging on a vulnerability.

In most business contexts, the risk of each particular harmful outcome is not all that high. The costs of risk mitigation, on the other hand, may be very high. Examples of the kinds of costs involved include:

- the time of managers, for planning and control;
- the time of operational staff and computer time, for regular backups;
- the loss of service to clients during backup time;
- additional media, for storing software and data;
- the time of operational staff, for training;
- duplicated hardware and networks; and
- contracted support from alternative 'hot-sites' or 'warm-sites'.

Risks have varying degrees of likelihood, have varying impacts if they do happen, and it costs varying amounts of time and money in order to establish safeguards against the threatening events or against the harm arising from a threatening event. The concept of `absolute security' is a chimera; it is of the nature of security that risks have to be managed. It is therefore necessary to weigh up the threats, the risks, the harm arising, and the cost of safeguards. A balance must be found between predictable costs and uncertain benefits, in order to select a set of measures appropriate to the need.

The aim of risk assessment is therefore to determine the extent to which expenditure on safeguards is warranted in order to provide an appropriate level of protection against the identified threats.

1.8.5 Risk Management Strategy and Security Plan

A range of alternative approaches can be adopted to each threat. These comprise:

- **Proactive Strategies**. These are:
  - Avoidance, e.g. non-use of a risk-prone technology or procedure;
  - Deterrence, e.g. signs, threats of dismissal, publicity for prosecutions;
  - Prevention, e.g. surge protectors and backup power sources; quality equipment, media and software; physical and logical access control; staff training, assigned responsibilities and measures to sustain morale; staff termination procedures;
- **Reactive Strategies**. These are:
  - Detection, e.g. fire and smoke detectors, logging, exception reporting;
  - Recovery, e.g. investment in resources, procedures/documentation, staff training, and duplication including 'hot-sites' and 'warm-sites';
  - Insurance, e.g. policies with insurance companies, fire extinguishing apparatus, mutual arrangements with other organisations, maintenance contracts with suppliers, escrow of third party software, inspection of escrow deposits;
- **Non-Reactive Strategies**. These are:
  - Tolerance, i.e. 'it isn't worth the worry' / 'cop it sweet';
  - Graceless Degradation, e.g. siting a nuclear energy company's headquarters adjacent to the power plant, on the grounds that if it goes, the organisation and its employees should go with it.

Devising a risk management strategy involves the following:

- selection of a mix of measures that reflects the outcomes of the preceding threat and risk assessments. The measures need to comprise:

  - **technical safeguard**s. These are variously of a preventative nature, support the detection of the occurrence of threatening events, enable the investigation of threatening events, and monitor the environment for signs of possible future threatening events. and
  - **policies and procedures**. These are organisational features, in the form of structural arrangements, responsibility assignment, and process descriptions;
- formulation of a **Security Plan**, whereby the safeguards and the policies and procedures will be put into place;
- **resourcing** of the Security Plan;
- devising and implementing **controls**, to detect security incidents and investigate and address them, and to monitor whether that all elements of the Security Plan are in place and functioning;
- embedment of **audit processes**, in order to periodically evaluate the safeguards, the policies and procedures, the actual practices that are occurring, and the implementation of the planned controls.

1.8.6 Security Plan Implementation

The process of implementing the Security Plan must be subjected to strong project management. Policies need to be expressed and communicated. Manual procedures need to be variously modified and created, in order to comply with the strategy and policy. Safeguards need to be constructed, tested and cutover.

Critically, implementation of a Security Plan also requires the development of awareness among staff, education in the generalities, and training in the specifics of the attitudes and actions required of them. This commonly involves a change in organisational culture, which must be achieved, and then sustained.

1.8.7 Security Audit

No strategy is complete without a mechanism whereby review is precipitated periodically, the need for adaptation detected, and appropriate actions taken. To be effective, audit must be comprehensive, rather than being limited to specific aspects of security; and it must follow through the entire organisation and its activities rather than being restricted to examinations of technical safeguards. Needless to say, this is heavily dependent on real commitment to the security strategy by executives and managers.

1.9 Information Security Tools, Standards and Protocols

A range of tools have been devised to assist in information security. In some cases, they are general-purpose safeguards, intended to be implemented by multiple organisations in order to provide protections against particular kinds of threats. In other cases, they are tool-kits rather than tools, devised as means whereby specific-purpose safeguards can be conveniently developed. Examples of tools include:

- **tools to assist with organisational safeguards**:
  - checklists for assessments of threats, vulnerabilities and risks;
  - checklists of safeguards;
  - guidelines for the design of safeguards, such as password selection;
  - checklists of security alert lists
  - checklists of the sites from which software fixes, patches and replacement versions can be downloaded
- **internal systems security tools**:
  - means of encrypting and decrypting data in storage;
  - means of inspecting for viruses on disk, and eliminating them;
  - means of examining and analysing log files;
  - audit tools for internal security (e.g. COPS, Tiger);

- means of checking the integrity of systems and application software (e.g. Tripwire);
- means of checking the vulnerability of systems software and endeavouring to address them (e.g. Solaris ASET, Titan, Bastille Linux);

- **networking security tools**:
  - access control tools, enabling the specification of privileges and groups, creating user accounts, and administering user accounts and passwords;
  - programs to access remote computers securely, e.g. ssh (`secure shell');
  - means of encrypting and decrypting messages;
  - packages to support private-key management;
  - tools to check digital certificate validity;
  - means of monitoring traffic to and from individual workstations;
  - means of filtering content arriving from remote computers (e.g. banner ad filters, virus detection tools, and cookie managers);
  - means of blocking unauthorised traffic between internal devices and external networks (`firewalls');
  - intrusion detection software (IDS);
  - audit tools that assist in testing external security, e.g. the Security Administrator Tool for Analysing Networks (SATAN).

Particularly in contexts in which interaction between networks is involved, commonality is important. Standards have been negotiated and published, and some categories of tools need to be compliant with them. In the area of electronic communications, standards are expressed in the form of protocols which connected devices need to comply with. Examples of **security standards and protocols** include:

- **SSL/TLS:** Secure Sockets Layer (SSL) is a protocol that provides an overlay of `channel encryption' over standard web-transmissions that use the http protocol. SSLv3 is implemented in all mainstream browsers (SSL 1996). Transport Layer Security (TLS) is a more recent enhancement to SSL (RFC2246 1999, RFC2487 1999, RFC2595 1999). In principle, SSLv3 and TLS also support two-sided authentication of both server and client. In practice, they are usually used for weak, one-sided authentication, with clients not providing certificates, and servers providing only weak evidence of their identity;
- **IPSec:** Internet Protocol Security (IPSec) is a series of standards and guidelines for the protection of data transmitted over the Internet (RFC2411 1998). They addres encryption, authentiation, integrity and replay protection, and key management through the Internet Key Exchange (IKE) standard (RFC2409 1998). IPSec has provided a mainstream way in which tunnelling can be performed, and Virtual Private Networks (VPNs) run over the open public Internet;
- **X.509v3:** This is a standard for the format of digital certificates (X.509 1997). It was originally conceived to operate within the context of X.500 directories, but has been widely applied independently of them. PKIX is a standard for using them on the Internet;
- **AADS:** The Account Authority Digital Signature Model (AADS) is a cut-down variant of conventional digital signature processes, applicable to communications among parties that have well-established relationships (i.e. already have `accounts' with one another), and who have already received and stored one another's public keys (Wheeler 1998). This obviates the need for public keys and key certificates to be transmitted with each message, and thereby avoids some of the problems inherent in X.509;

- **SDSI:** Simple Distributed Security Infrastructure (SDSI) is another alternative approach to the conventional X.509 scheme (SDSI 1996-). SDSI abandons the X.509 nirvana of a single, global name-space. A certificate associates a public key (and hence a key-pair) to an entity that only the CA knows, and no warranties are provided by the CA to the recipient of the message as to who the keyholder is. It is up to the relying party to build up an image of the sender based on its successive interactions with the holder of that key;
- **P3P:** Platform for Privacy Preferences (P3P) is a protocol for the communication of privacy policy statements by servers on behalf of service providers, such that clients, on behalf of consumers, can decide whether or not to deal with that provider (Clarke 1998);
- **SSH:** Secure Shell (SSH) is a de facto standard protocol for secure logins, file transfer and remote execution of programs (like telnet, ftp and rlogin with strong crypto). It can also be used as a transport for other protocols.

In an increasingly mature marketplace, a significant proportion of a Security Plan comprises the selection of tools that are compliant with relevant standards and protocols, and the specification of ways in which their potentials are to be applied in order to achieve safeguards desired in the particular context.

1.10 Conclusions

Information security is important, challenging, and multi-faceted. It involves organisational safeguards as well as technical safeguards. It cannot be approached using naive military ideas about 'absolute security'. Instead a 'risk-managed' approach has to be adopted, and costs and inconvenience traded-off against security. And it requires vigilance, because security schemes suffer from entropy, i.e. they run down very quickly unless they are maintained.

Exercises

1. Define Information Security ? Discuss the potential risks to Information Systems.
2. Explain the various benefits of good Information Security System in a Business environment.
3. Write notes on
   a) Internal Information Security Threats
   b) External Information Security Threats
4. Explain the Information Security Architecture ?
5. Discuss the Information Security process in detail.
6. Explain the various Information Security tools. With the Standards & Protocols.