7 Information Security Management

7.1 Introduction

From the business perspective information has its value and thus has become an *asset*. Therefore just as any other type of business assets, it needs to be protected. Businesses are continuously exposed to an ever increasing range of *threats* to their information. Ranging from human error, equipment theft and physical destruction, modern threats to information security extend to sabotage, fraud, vandalism and terrorism. Furthermore, risks to modern organisations grow as companies operate in a complex interconnected world where the pace of evolving technologies is staggering.

The burning question is how a business can secure its information assets? The term *information security* refers to safeguarding or protecting information assets from threats that may harm valuable information. In order to protect information, the *infrastructure,* which supports information, including communication networks, systems and processes relevant to managing information, needs to be protected as well.

Information security is often regarded as the level of confidence of being protected or bringing risks to a minimum via establishing of controls and security measures. Besides hardware and software controls, businesses address information security through policies, procedures and organisational structures. In order to protect and derive maximum value from their information assets, businesses need to develop and continuously monitor comprehensive security controls. In this chapter we will discuss best practice approaches and international standards explaining what a business can do to protect its information assets, but firstly it is important to make the business case for information security management and go over some essential terminology.

Information security also implies the existence of *vulnerabilities* (known or yet unknown) in a system which impose risks to information assets. Vulnerability pertains to a weakness/flaw in a system making an attack or an unintentional compromise of data possible. Existence of vulnerabilities in a system leads to risks, for example, if a bug (or an error) in an application is not fixed (or patched) the application is at risk from hackers exploiting this vulnerability. As shown in figure 1 information assets can have various vulnerabilities which may ultimately result in compromises of valuable business information. The term *compromise* indicates that an information asset was impacted in an undesired manner. As the result of compromises the state of information may change (e.g. transactional records in a corporate database can be fully or partially destroyed by malicious code attack), or remain intact (e.g. credit card information stolen by a hacker in the wireless network of a department store); however in both cases information assets are maliciously impacted, i.e. compromised, through attacks exploiting existing vulnerabilities in information systems.

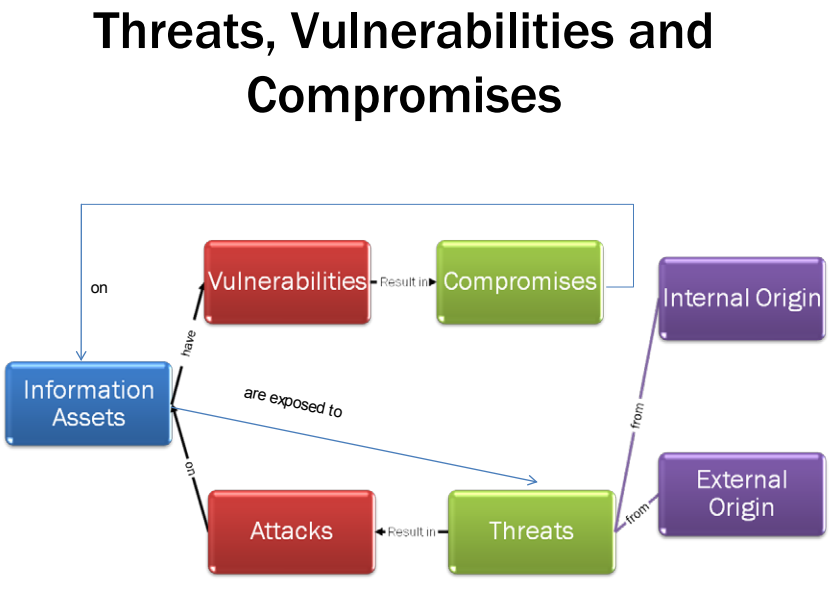

Figure 1. Threats, Vulnerabilities and Threats to Information Assets.

Information is constantly exposed to *threats* of either internal (including poorly trained personnel, espionage, human error, etc.) or external origin to organisations (such as malicious code, hacking, denial of service attacks and many, many others). Whether a threat results in a successful *attack* on information largely depends on existing vulnerabilities in information systems. If information is secured, thereby bringing vulnerabilities to a minimum, attacks threatening information assets are likely to be detected and prove unsuccessful.

Actions taken to protect information or a system from threats and ensure its security are known as *countermeasures*. They are deployed to minimise risks of attacks and to reduce vulnerabilities. Generally, security measures may be classified by their nature into physical and logical. *Physical security measures* safeguard information assets by preventing physical theft, loss or damage of equipment where data is stored or processed. *Logical security measures* pertain to soft methods of information protection. For example, data stored on a company's database server is usually protected by logical countermeasures such as encryption and access to it is open only to authorised employees. A range of methods for ensuring logical security may be employed for protection of a company's database. On the other hand, corporate data may be compromised by someone breaking into the building, stealing data directly from hard disks or damaging corporate hardware. To prevent damage or theft of the database server hardware physical access into the area may be restricted by locks, alarms and other physical measures. In this unit, we will be principally referring to logical security measures although most modern security control frameworks comprehensively address both logical and physical information security management.

Measures introduced to guard information against attacks are often referred to as *controls*. For example, amount of overtime hours entered by an employee into a company's financial system is subject to verification against the maximum overtime hours possible. This represents an internal control ensuring that correct information is entered into the system and preventing abuse. Controls intrinsic to a specific organisation are called *internal controls* as they are located within the boundary of an organisation. We also need to draw attention to the fact that control is not an event, it is a business process itself. If it is a process, then it has specific objectives (e.g. minimising risks posed by internal or external information security threats) and is managed by people (e.g. managers, IT department, etc.). Hence the threefold nature of the information security subject encompassing logical/physical countermeasures, people and processes in a business.

The Internet underpins a considerable amount of business activity, radically changing traditional business models and enabling new global economic opportunities. It has transformed the way in which people access information, socialise and entertain themselves. It has enabled a positive transformation of society and the very existence of the knowledge economy. However, the technology behind Internet communications and the general lack of an in-depth understanding of how it works by the majority of users creates significant risks. The invisibility of Internet technology to end users generates risks and facilitates criminal activity including industrial espionage, threats to business continuity and risks of services failure. In the next section we will look into the types of Internet risks and consequences of information security failures.

7.2 Internet Security Threats: Known, Unknown and Predicted

"It takes many good deeds to build a good reputation and only one bad to lose it."

Benjamin Franklin

Managing information security measures is a complex task. One may notice that it is impossible to bring information risks to zero as it is impossible to know all information system vulnerabilities or predict threats to information which may emerge in the future. When a security breach occurs, it may go unnoticed for quite sometime, however its consequences to business may be enormous. According to research from Weber Shandwick (2007) it may take a business up to 3.6 years to recover the damage to its reputation. Information security breaches are frequently becoming the cause of damaged reputation and loss of consumer or trading partner confidence.

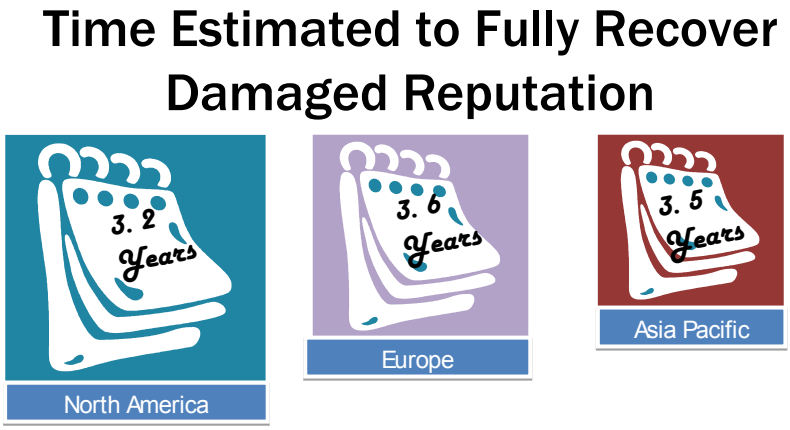

Figure 2. Reputational Risks: Hard to Calculate (Weber Shandwick 2007).

Threats to information assets, increasingly originating on the Internet, are becoming more sophisticated, more frequent and more dangerous. Teenage hackers of the past have given their place to organised cybercriminals who aim at capitalising on theft, putting companies out of business, or even committing terrorism.

A major cause of cybercriminal activity on the Internet, whether sending spam email or perpetrating a denial of service attack, is caused by the distribution of malware on individual computers. Malware, or malicious code, used to be categorised into *viruses* which propagate by means of legitimate Internet traffic such as emails and *worms* which infect computers without human interference. As the threats of malware continue to rise, both terms are being used now almost interchangeably. Malware origin can still include email, or interconnection to other machines and storage devices – but an important new venue of infection is from browsing a website, intentionally designed to infect other machines. Malware now comes in all shapes and sizes initially fuelled by intentions of irresponsible individuals to gain celebrity status among peers. The notorious "ILOVEYOU" worm attack could serve as such example as the malware was created in by a disaffected student in the Philippines in 2000. Today most frequently the development of malicious code is profit-driven, i.e. intends to leverage infected computers in order to make money. MPack, exploiting client-side vulnerabilities of individuals visiting a compromised web-site, was one of the newly emerged types of malware. It was professionally developed, supported and available commercially in 2007. Increasingly, malware is being designed to be undetected for the machine's owner and capable of spreading in a sublime manner. The purpose of a malicious code can be to search the hard disk of a compromised computer to steal keys, passwords for systems and other confidential information. To enable continuous capture of secret information, malware may install a *keylogger* (a programme which records any keyboard activity including capturing websites visited and passwords used for information systems or online banking), permitting the criminal to compromise personal and corporate information.

Infecting computers with malicious code is frequently done in order to create a *botnet* consisting of individual computers known as *zombies.* A *botmaster* makes the infected computers operate as a network with a malicious purpose, such as sending spam, hosting an illegal website or perpetrating other types of attacks. Owners of the individual computers are often unaware of the illegal activity taking place, although the origin of the malicious actions can be traced back to the unsuspecting victims.

The intrinsic design of the Internet allows the increasing of *distributed denial of service attacks (DDoS)*. In this case, many computers running malicious programs or an entire botnet directs communication traffic to a single web server, in which case the latter becomes overloaded with traffic and fails to respond to legitimate requests. In most cases DDOS are not aimed at individual computers but threaten the integrity of business networks, government and domain names. Although historically networks are built with an enormous over-capacity to accommodate such traffic, cases of DDoS attacks frequently affect business continuity due to incapacitating their Internet operations.

In recent years online financial services have been affected by an increasing number of phishing attacks. For the first time the term *phishing* was used in 1996 in relation to the incidents of passwords disclosed as a result of email deception of America Online (AOL) customers. It appears that recently there has been a shift towards phishing by means of misrepresentation of legitimate websites of financial institutions, online storefronts or service providers by their illegitimate replicas. For a regular consumer such fraudulent websites are rather difficult to distinguish from the original ones. The figure below illustrates how close a phishing website could appear to the original one.

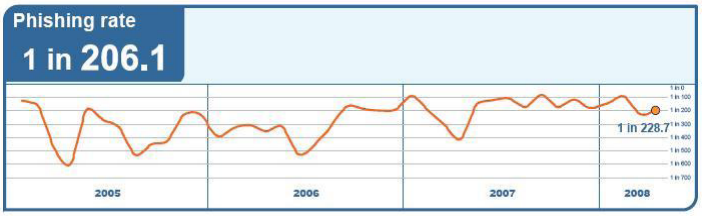

Figure 3. Phishing Rates 2005–2008 (MessageLabs 2008)

Again the technical aspect of such impersonation is rather unsophisticated and relies on the unsuspecting victims giving up confidential information to the fraudulent site instead of the legitimate financial institution or storefront. The phisher's intention is to angle for confidential information that the victim has access to, including PayPal and bank account numbers, username and passwords, debit and card numbers. Some attacks may be disguised as alerts about payment due or data verification. The damage cause by phishing attacks is growing. In 2005 in the UK the losses caused by phishing attacks amounted to £504 million. The United States damage due to phishing reached nearly one billion dollars. According to a report from MessageLabs (2008) one in 206.1 emails (or .49%) comprised a phishing attack and numbers are going up. As shown in figure 3, when compared to the to the proportion of the all the threats delivered through email traffic such as viruses and worms, the number of phishing emails reached 87.1% of all email-borne malware. Phishing is a global trend in Internet attacks with most United Kingdom banks reporting growing losses from direct online banking fraud reaching £33.5 million in 2006. Although considerably smaller than online banking fraud figures for same years in the United States, the United Kingdom trend continues to rise from £12.2 million in 2004, £23.2 million in 2005 and growing steadily.

Traditional countermeasures such as anti-virus software (which determine whether a piece of code is known to be malicious) continue to be used, although they no longer present a silver bullet solution as they once did. Faced with the escalating numbers of new malware the anti-virus companies have joined forces. Collectively they prioritise, process and shut down the most dangerous malware and the most widespread. For instance, Symantec Corp. employs 40,000 sensors monitoring Internet activity and gathering malicious code reports. They have observed that the current security threat landscape is characterised by the following:

- Increased professionalised and commercialisation of malicious activities
- Threats that are increasingly tailored for specific regions
- Attackers targeting victims by first exploiting trusted websites
- Convergence of attack methods (Source: Symantec Internet Security Threat Report 2007).

7.3 Brand Protection on the Internet

Brand protection, encompassing trademarks and intellectual property, is becoming increasingly challenging in the digital world. The global reach of the Internet and exponential growth of online transactions make brand protection immensely more complex in the modern world. According to Forrester Research in 2007, $175 billion worth of goods and services were purchased online. In 2008 this figure reached $204 and is predicted to grow further (MarkMonitor 2007). Unfortunately, sales of counterfeit goods are expected to rise as well. Fraudsters are eagerly exploiting such benefits of the Internet as global reach, anonymity, ease of replication of images, trademarks and intellectual property from original brand owners. The impact of Internet sales of counterfeit goods pose considerable threats to a number of stakeholders including:

- Brand owners experiencing loss of revenue and market share, erosion of brand equity, loss of customer trust.
- Retailers and distributers affected by the profit margin erosion and brand value reduction.
- Customers inadvertently deceived by fraudulent goods lose trust in genuine articles, as well as may be exposed to health and safety risks imposed by lower quality products.
- Governments impacted through the loss of tax revenue, bearing increased costs of enforcement and surveillance.
- Workers concerned about job losses.

Internet sales of fraudulent goods produce a multitude of concerns for corporate brand owners beyond major losses of revenue. The range of problematic issues include product liability lawsuits, inability to recover research and development costs of products, compliance problems as government guidelines call for disclosure of threats to revenue including those caused by counterfeit sales.

To mitigate threats of online fraud and timely uncover violations strong control measures must be in place to address counterfeit issues in a proactive manner. An approach to online brand protection depicted in figure 4 illustrates a holistic approach to ensure security or restoring confidence in online sales channels.

The approach of online brand protection comprises of three phases as follows (MarkMonitor, 2007):

Prevention of Online Channel Abuse.

For established brands it is important to prevent online abuse by managing domain name registrations which may impinge upon a company's brand.

- Continuous monitoring of domain names, defensive acquisition of domain names owned by unfamiliar third parties are among the necessary actions for management of online brands.

- Conducting a gap analysis of domain names and identification of potentially harmful domain names which may be used for phishing attacks or divert traffic from the branded domain.

Detection of Online Channel Abuse.

Online channel abuse may come from a multitude of sources including auction sites, high volume B2B exchanges, general electronic storefronts, etc. – Detection of online channel abuse is carried out by automatic applications scanning through online channels for counterfeit goods specific to the corporate brand.

- Scanning for links, images, scam emails and domain names luring consumers to counterfeit sites constantly gathers information from the Internet traffic.

- Having detected the origin of the brand abuse, it is possible to identify the offenders.

Response to Online Channel Abuse.

- Continuous monitoring of the Internet provides sufficient information related to fraud to respond to brand infringement.

- These actions include sending Cease and Desist (C&D) letters, delisting requests to auction sites as well as warnings. Corporations increasingly emphasise significance of their brands and press for legal actions against the offenders.

Proactive Brand Protection Approach

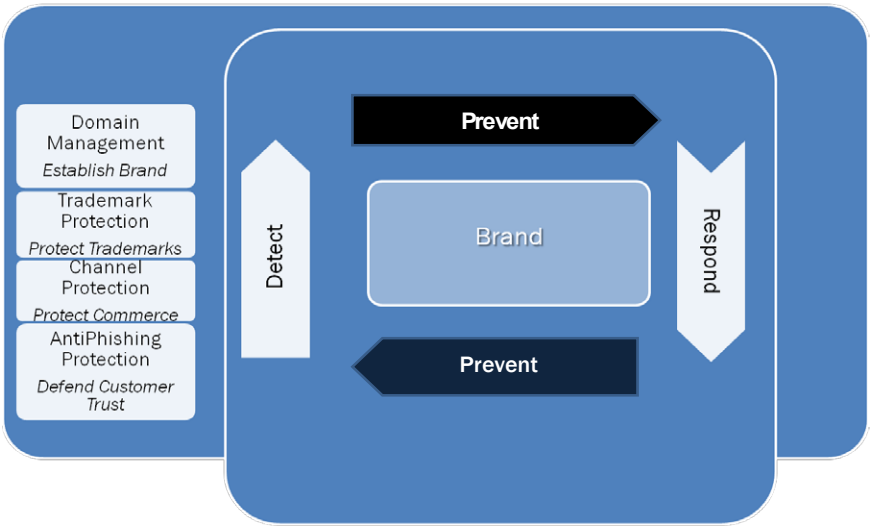

Figure 4. Holistic Approach to Online Brand Protection.

The process of online brand protection is rather complex. Corporations, especially Fortune 100 companies, tend to outsource prevention of online channel abuse. Service providers, such as MarkMonitor delivering solutions to 50 from the Fortune 100 companies, execute all phases of proactive brand management using automated methods.

7.4 Compliance Issues

There are two main reasons why information assets need to be protected. First being the ever increasing probability for information to be compromised either externally or internally, intentionally or accidentally. The second reason rests with the regulatory requirements, the necessity for compliance with legislation concerning information collection, use and protection. Violation of regulation may be detrimental to business not only in legal terms, but also lead to significant damage to reputation and image. For today's business it is imperative to have established controls in place which ensure compliance with the requirements set forth by regulatory bodies and government.

A recent security breach at one of well-known companies (further referred as Company A) was closely followed by US government and undoubtedly caused a great deal of financial and reputational damage to the business. A laptop containing customer records was lost by one of the Company's employees. This is an extract from the Attorney General's Office (2006) letter to Company A:

Please provide written answers to the following questions:

Prior to the breach of this data, what measures did Company A take to safeguard individuals' personally identifying information;

Please indicate if and when Company A first notified criminal authorities about this data breach;

Please describe in detail how Company A laptop containing this personal data was compromised;

Please describe in detail the categories of information compromised by the data breach from Company A laptop, such as, but not limited to, name, address, phone number, date of birth, driver's license number or other personal information;

Please describe all steps that Company A has taken to track down and retrieve the personally identifying information;

Please identify all steps Company A has taken or will take to contact and warn consumers that their personally identifying information may have been compromised, including but not limited to, when and how Pfizer first notified consumers of this data breach;

Please identify what, if any, regulatory scheme Company A follows when responding to security breaches;

Please describe Company A's general corporate policies regarding securing computer systems, facilities, and personally identifying information.

These are some difficult questions to answer. The business impact of information security breaches is significant and definitely measurable in financial terms. Without a structured assessment of the company's business risks and establishment of rigid controls an enterprise may be at higher risk from both external threats and regulatory compliance.

In the UK the Data Protection Act (1998) and Human Rights Act (1998) set out the legal framework to safeguard privacy and establish the legal basis for the management of information and the right of the individual to privacy. The Freedom of Information Act (2000) provides the public 'right to know' in relation to public bodies.

In the US as a reaction to the significant number of corporate scandals related to financial information reporting in the late 1990s government instituted the Sarbanes-Oxley Act. This Act, relevant to all publicly traded companies in the US, stipulates how corporate financial information is to be reported and provides relevant Corporate Governance regulations. Principally, the Sarbanes-Oxley Act requires companies to have internal control systems to ensure disclosure of accurate financial information. As companies increasingly rely on IT for secured storage, accurate processing and management of financial data and documentation, enterprises need to establish effective IT controls, identify and assess information risks effectively. Some of the most widely recognised frameworks addressing IT governance and information risks management are covered in the next section of this unit. Their objectives are to ensure that management internal control activities are in place in order to draw value from corporate IT resources, achieve compliance and mitigate IT risks in an enterprise.

7.5 Frameworks for Control and Security: COBIT®, ITIL®, and ISO 27002

Over the years three rather different, but widely accepted, IT governance frameworks have been developed. They are COBIT®, ITIL® and ISO 27002. Each of these frameworks was developed in a different country and by a third party, i.e. these frameworks are vendor-independent. Although any of these frameworks may not serve as a silver bullet to resolving information security risks, each has its fortes in IT governance.

Control Objectives for Information and related Technology, or COBIT ® is increasingly popular framework of practices for IT, internal information controls and risks mitigation. COBIT, developed by America's IT Governance Institute, aims to facilitate implementation of enterprise-wide governance of IT. Its objective is to help enterprises to integrate information technology with business objectives and strategic management, to harvest value of their information assets and capitalise on IT in an increasingly competitive business and stringent regulatory environments. COBIT is a process oriented framework, which provides management guidelines for monitoring and evaluating an enterprise's IT resources. The framework offers tools responsive to the management needs to control and monitor enterprise's IT capability for its various business processes. The best practice approach provided by COBIT includes such tools as:

- Performance drivers for IT
- Best practices for IT processes and relevant critical success factors
- Elements for performance outcome measurement
- Maturity models instrumental for decision making over capability improvements.

According to COBIT there are 34 IT processes in an enterprise, every process is assigned a level of maturity on a scale of 0–5 from non-existent to optimised or best practice. The maturity levels are used for benchmarking of IT capabilities. IT processes are grouped into four domains, such as:

- Plan and Organise;
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate.

For each COBIT process a set of control objectives is assigned. For instance, a process *Ensure System Security* which belongs to the domain of *Delivery and Support* will have an objective of *Minimise the impact of security vulnerabilities and incidents*. This objective can be assessed by the number and severity of projected and actual information security breaches, % of compromised cryptographic keys compromised and revoked, number of access rights authorised, revoked, changed, etc. Table 1 summarises selected processes and general control objectives outlined in the COBIT framework.

Domain	High Level Control Objectives
Delivery and Support	Ensure Continuous Service
	Ensure System Security
	Educate and Train Users
	Manage Service Desk and Incidents
	Manage Problems
Monitor and Evaluate	Monitor and Evaluate IT Processes
	Monitor and Evaluate Internal Control Systems
	Ensure Regulatory Compliance
	Provide IT Governance

Table 1 Selected Control Objectives in COBIT.

COBIT takes a best-practice approach to assist managers in establishing appropriate internal controls and aligning control needs, business risks and IT capabilities. The framework ensures that internal control systems support the enterprise's business processes through identification and measurement of individual control activities. These activities comprise of management policies/procedures, business practices and organisational structures.

In addition to other risks that an enterprise can face, COBIT deals with IT security. COBIT Security Baseline comprehensively covers risks of IT security and provides key controls for mitigating technical security risks. As discussed earlier in the unit enterprises, especially trading in the US, have to comply with stringent regulations. COBIT has established itself as the most adopted internal control framework to achieve compliance with the Sarbanes-Oxley Act.

ISO27002: Code of Practice for Information Security Management.

ISO 27002, the updated version of ISO 17799 in 2007, is a *Code of practice for information security management*. It provides the general principles for planning, implementing and improving information security management for businesses. The standard, released by the International Standards Organisation in Geneva, establishes the guidelines on information security control objectives and focuses on information in its various forms.

It is worth mentioning that ISO 27002 addresses security of information in possibly all of its formats including electronic files, paper documents, recordings/media and communications. The standard is comprehensive enough to group information in context of communication into conversations (telephone, mobile, face to face) and messages (email, fax, video and instant messaging).

ISO 27002 suggests initiating implementation of information security management by gathering company's information security requirements. This is done through a process consisting of the following steps:

1. **Perform risk assessment** – aimed at identifying vulnerabilities and threats, as well as establishing their likelihood of them causing an information security breach and its consequences to business objectives.
2. **Study legal requirements** – this step includes addressing the legislative and contractual requirements of all business stakeholders including suppliers, partners, etc. and ensuring that the regulatory requirements specific to the business are met.
3. **Scrutinise requirements internal to business** – through examination of information management processes, methods and practices inside the organisation it is possible to identify information security needs and requirements unique to the organisation.

Having examined the company's information security needs and requirements, ISO 27002 recommends developing/improving the business's *information security program.* This program is built from the best-practices provided by ISO 27002 by selecting practices which meet information security requirements unique to the company. It is recommended to establish core security practices such as:

- "Allocate responsibility for information security
- Develop an information security policy document
- Make sure applications process information correctly
- Manage information security incidents and improvements
- Establish a technical vulnerability management process
- Provide security training and awareness
- Develop a continuity management process".

The basis of the legal practices in a company's information security program must include at least:

- "Respect intellectual property rights
- Safeguard organisational records
- Protect privacy of personal information" (*ISO 27002: 2005 Introduction)*

ISO 27002 addresses objectives of information security management and recommends controls which should be used to achieve these objectives. For example, the section concerned with *Information Security Incident Management* includes an objective, *Make sure that information system security incidents are promptly reported.* Relevant controls corresponding to this objective will include, *Report information security events using the appropriate management reporting channels* and *Make sure that security events are reported promptly.* In addition to the set of objectives and controls ISO27002 provides notes and guidelines on how to implement controls and apply objectives. For the objective discussed above one of the guidance notes is *Establish a formal information security event reporting procedure.*

The set of best practices comprehensively covers a broad range of management areas from Human Resource Security Management to Information Security Incident Management. Any business organisation is not compelled to implement the entire set of best practices provided in ISO 27002 – only specific practices which help address information security risks or meet a compliance requirement relevant to the organisation need to be applied.

Information Technology Infrastructure Library or ITIL® emerged in recognition to an increasing dependence of enterprises on information and IT in order to meet their business needs. Developed by the UK Office of Government Commerce, ITIL comprises of a comprehensive set of good practice documentation for managing IT infrastructure, development and delivery of quality services. Through the use of best practices ITIL provides a systematic approach to the IT Service Management. ITIL has been highly acclaimed and adopted by such large organisations as Barclays Bank, HSBC, British Airways, MOD, etc.

ITIL has focuses on the Service Management and IT support for operational processes and their continual improvement. Over the years since the earlier versions of ITIL it has emerged that Service Management is a wider concept than just supporting the end-product. The later version (version 3) of ITIL now addresses the Service Lifecycle including Strategy, Design, Transition and Operations.

ITIL covers Security Management as a process of embedding information security into organisational management. ITIL Security Management is largely based on the ISO 17799/ISO 27002 standard and treats information security as the process of safeguarding information from risks. It addresses the need to minimise information security risks, often concentrating on the physical security of information assets, in order to achieve and improve IT service management. Specifically, information security breaches and attacks can negatively impact service operations and continuity thereby in ITIL context, degrade service value and benefit.

Various IT control frameworks have emerged over the past decades, enabling organisations to establish robust internal security controls. Their primary objective is to provide a structured system for any business to establish a system of controls as complete as possible fully addressing corporate business processes and infrastructure. The frameworks described here offer substantially different approaches to control and security. However, they are flexible enough to allow any business, from small companies to global enterprises, to adapt and implement only selected components of the framework to the specific needs of a business.

7.6 Exercises

1. Exercise: At a high level view COBIT, ITIL and ISO27002 have a lot in common. However, each of the security and control frameworks discussed in this unit has its unique characteristics. Identify and discuss similarities existing between these frameworks. Summarise and discuss with your colleagues specific differences between them. The following categories may help in your comparative analysis of the frameworks: *technology, implementation, environment, personnel, controls, processes and metrics*.

2. Exercise: Following a number of information security incidents, the UK government conducted a review of its data handling procedures. In a small group, or individually, research some of the news headlines related to data loss incidents. Discuss with your colleagues what security control objectives should be in place to avoid such incidents of data loss in the future.

Compare your suggestions to the information security agenda suggested in the following report **Cabinet Office (2008)** ***Data Handling Procedures in Government: Final Report*** http://www.cabinetoffice.gov.uk/~/media/assets/www.cabinetoffice.gov.uk/csia/dhr/dhr080625%20pdf.ashx

Finally, what security and control framework(s) are recommended to be implemented by this report?

3 Exercise: Research how one of the Fortune 100 companies protects its brand online. Or you may choose one of the following companies:

- Toyota
- Lloyds tsb
- NatWest
- Sony

Identify measures the company of your choice takes to protect and manage its brand online. Collect information about possible threats pertaining to brand that the company experienced in the past.

Also, attempt to list possible benefits and savings obtained through online brand protection. Share your findings with your class colleagues or on the discussion forum as directed by your instructor.