CHAPTER 7 Human Factors

LEARNING OUTCOMES

By the end of this chapter, you should be able to:

1. Identify the security standard, policy and guideline for best practice;
2. Determine the risk management process and the role of risk management team;
3. Identify the ethical issues in computer security and the rights of the employee/ employer;
4. Examine the importance of security awareness; and
5. Conduct the security audit and control.

INTRODUCTION

Observe the article taken from the Internet below.

Life without the net

Boston
October 8, 2004

Without the internet, Russ Nelson was lost - literally. As a college student in Chicago, he usually finds his way to new places by checking websites such as MapQuest, but when he agreed to stay offline for an experiment, he ended up "just wandering around," he says.

For two weeks, Nelson and 27 other Americans with broadband connections kept diaries about how this internet deprivation affected their daily lives. Yahoo! Inc and the OMD media agency commissioned the study to give marketers a deeper understanding of people's dependence on email, websites, and other internet-based tools.

They also asked 1000 online households how long they could do without. Half said fewer than five days.

The study offers a fascinating glimpse into how society is grappling with the effects of a relatively new technology.

On one web forum, reaction to the study divided into two camps: one that reviles people who feel helpless when they can't get online and another that proudly declares its dependence on such a convenient medium.

But experts caution against drawing too many conclusions from such a small sample. Of the 88 per cent of Americans who say the internet plays a role in their daily lives, only one-third say it's a major role, according to research by the Pew Internet & American Life Project in Washington.

Two-thirds are just starting to blend the internet into their routines.

"They can take it or leave it in a sense, and transfer what they do (online) to the old way of doing things," says Deborah Fallows, a senior research fellow at the Pew project. It would be misleading "to say that all internet users can't live without it."

Source: http://www.theage.com.au/news/technology/life-without-the-net/2004/10/07/1097089475913.html?from=moreStories

Based on the article, provide your feedback on life without the internet. Highlight your points on your feedback and share your opinions with the other students.

In today's information society, life without information and communications technology is almost inconceivable. For this reason, the protection of IT environments is gaining more and more importance. Changed legal requirements are also contributing to a higher awareness for IT security topics: directors are now personally responsible for omissions and inadequate risk prevention.

Work and business processes are increasingly based on IT solutions. For this reason, the security and reliability of information and communications technology gains all the more importance. The right IT security concept can assist you in building a solid basis for a level of IT security you can rely on. IT security plays a vital role in securing the information assets of organisations and businesses especially in today's global war against terrorism. Thus, the IT security policy, guidelines or procedures, and standards are designed to help organisation with this, providing a compact overview of the most relevant security safeguards Standardisation of IT security is the work of international standard bodies such as the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC).

7.1 STANDARDS AND POLICY GUIDELINES

Some organisations issue overall computer security manuals, regulations, handbooks, or similar documents. These may mix poicy, guidelines, standards and procedures, since they are closely linked. While manuals and regulations can serve as important tools, it is often useful if they clearly distinguish between policy and its implementation.

This can help in promoting flexibility and cost effectiveness by offering alternative implementation approaches to achieving policy goals. Familiarity with various types and components of policy will aid managers in addressing computer security issues important to the organisation.

Effective policies ultimately result in the development and implementation of a better computer security program and better protection of systems and information. A key element of any organisation's security planning is an effective security policy.

7.1.1 Security Standard

There is required that agencies adhere to common IT security standards in order to implement the Information Technology (IT) Security Policy, to protect IT resources, and to enable security audits of those resources. Common standards will help ensure that all agencies have an effective and secure environment for IT processing.

The protection of computer systems and related data in the most of the countries in the world requires an approach that results in implementation of a balanced, cost-effective application of security disciplines and techniques required by these standards.

Security standards define the processes, procedures, and practices necessary for implementing an agency-specific IT security program.

These standards apply to all IT activities, whether they are operated by or for an agency. They include specific steps that shall be taken to ensure that a secure IT environment is maintained and all agency systems provide for privacy and security of confidential information.

7.1.1.1 Malaysia Security Standard

Malaysia has adopted a few security standards such as shown in Figure 7.2.

A few security standards adopted in Malaysia

- ISO/IEC 17799 (information security management).
- TR 13335 (Guidelines for the Management of IT Security - GMITS).
- ISO/IEC 15408 (Common Criteria).

Figure 7.2: A few security standards adopted in Malaysia

The relationship between three of them is depicted as in Figure 7.3.

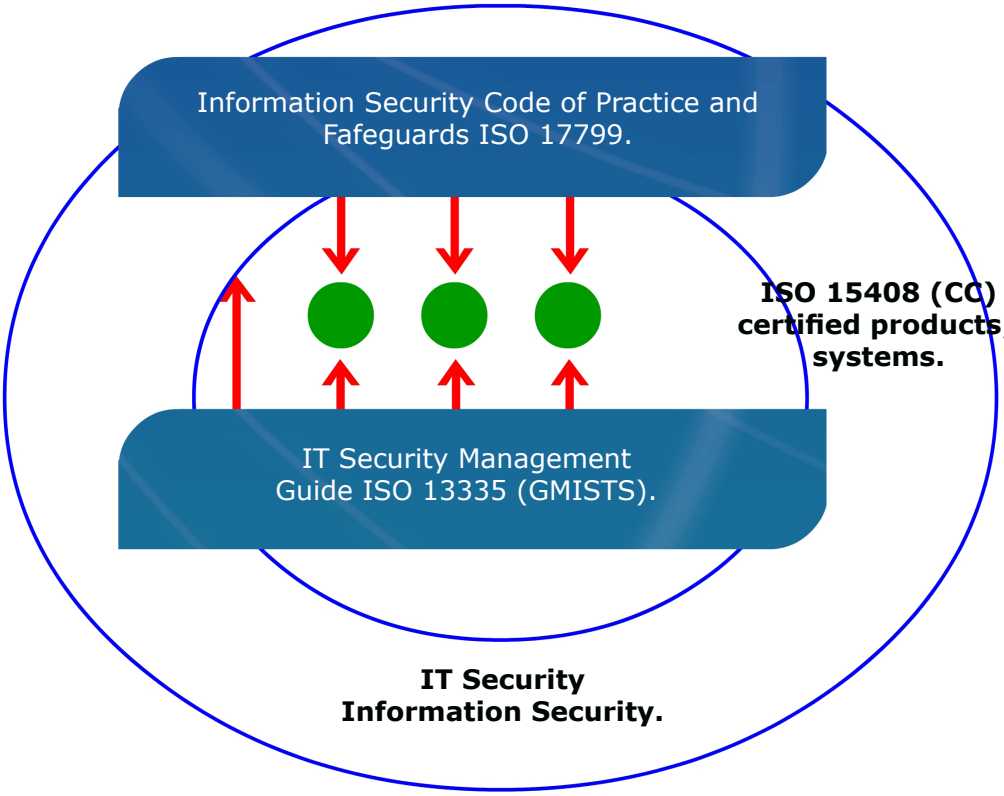


Figure 7.3: Relationships between security standards

However, in this section, it will only discuss about ISO/IEC 17799 as it is a detailed security standard. ISO/IEC 17799 is code of practice for information security management. It was adopted from BS7799 Pt 1. This standard provides a common basis for developing organisational security standards and effective security management practice. It used as a starting point for developing organisation specific guidelines for the management of information security. It is organised into 10 major sections, each covering a different topic or area as depicted in Figure 7.4.

Figure 7.4: Areas/topics covered in ISO 17799

From Figure 7.4 above, let's look into details the objective in each of the areas covered in ISO 17799 which were described in Table 7.1

Table 7.1: Areas/Topic Objectives

Areas/Topics Covered	Objectives
Responsibility Distribution	The objectives of this section are to counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.
System Access Control	The objectives of this section are: • To control access to information; • To prevent unauthorised access to information systems; • To ensure the protection of networked services; • To prevent unauthorised computer access; • To detect unauthorised activities; and • To ensure information security when using mobile computing and telenetworking facilities.

System Development and Maintenance	The objectives of this section are: • To ensure security is built into operational systems; • To prevent loss, modification or misuse of user data in application systems; • To protect the confidentiality, authenticity and integrity of information; • To ensure IT projects and support activities are conducted in a secure manner; and • To maintain the security of application system software and data.
Physical and Environmental Security	The objectives of this section are: • To prevent unauthorised access, damage and interference to business premises and information; • To prevent loss, damage or compromise of assets and interruption to business activities; and • To prevent compromise or theft of information and information processing facilities.
Compliance	The objectives of this section are: • To avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements; • To ensure compliance of systems with organisational security policies and standards; and • To maximise the effectiveness of and to minimise interference to/from the system audit process.
Personnel Security	The objectives of this section are: • To reduce risks of human error, theft, fraud or misuse of facilities; • To ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work; and • To minimise the damage from security incidents and malfunctions and learn from such incidents.
Security Organisation	The objectives of this section are: • To manage information security within the Company; • To maintain the security of organisational information processing facilities and information assets accessed by third parties; and • To maintain the security of information when the responsibility for information processing has been outsourced to another organisation.

Computer & Network Management	The objectives of this section are: • To ensure the correct and secure operation of information processing facilities; • To minimise the risk of systems failures; • To protect the integrity of software and information; • To maintain the integrity and availability of information processing and communication; • To ensure the safeguarding of information in networks and the protection of the supporting infrastructure; • To prevent damage to assets and interruptions to business activities; and • To prevent loss, modification or misuse of information exchanged between organisations.
Asset Classification and Control	The objectives of this section are: • To maintain appropriate protection of corporate assets; and • To ensure that information assets receive an appropriate level of protection.
Security Policy	The objectives of this section are to provide management direction and support for information security.

7.1.1.2 Benefits of Using the Standards

There are several advantages by using the security standard such as:

- Organisations in a better position to deal with and respond to malicious electronic and IT activities;
- Creates trust between business entities;
- Increased public confidence in local business organisations and government agencies;
- Be able to offer products and services to a world-wide market;
- Local IT security products/systems may be marketed internationally (more and more countries mandating CC certification); and
- Enhance national cyber defence capability.

7.1. 2 Security Policy

A key element of any organisation's security planning is an effective security policy. A security policy must answer three questions (see Figure 7.5).

Figure 7.5: The three questions that a security policy must answer

A security policy is a high level management document to inform all users of the goals of and constraints on using a system. A policy document is written in broad enough terms that is does not change frequently. The information security policy is the foundation upon which all protection efforts are built. It should be a visible representation of priorities of entire organisation, definitively stating underlying assumptions that drive security activities.

The policy should articulate senior management's decisions regarding security as well as asserting management's commitment to security. In order to make the policy is effective, it must be understood by everyone as the product of a directive from an authoritative and influential person at the top of the organisation.

7.1.2.1 Security Policy Purposes

Security policies are used for several purposes including the following:

- Recognising sensitive information assets.
- Clarifying security responsibilities.
- Promoting awareness for existing employees.
- Guiding new employees.

7.1.2.2 Security Policy Audience

A security policy addresses several different audiences with different expectation. Figure 7.6 shows the group of audience that consists of:

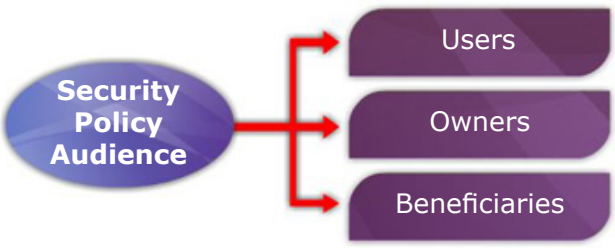


Figure 7.6: Security Policy Audience

From Figure 7.6, let us look into each of the audience in security policy in details.

1. Users

Users legitimately expect a certain degree of confidentiality, integrity and continuous availability in the computing resources provided to them. Although the degree varies with the situation, a security policy should reaffirm a commitment to this requirement for service.

User also needs to know and appreciate what is considered acceptable use of their computers, data and programs. For user, a security policy should define acceptable use.

2. Owners

Each piece of computing equipment is owned by someone and the owner may not be a system user. An owner provides the equipment to users for a purpose such as to further education, support commerce or enhance productivity. A security policy should also reflect the expectations and needs of owners.

3. Beneficiaries

A business has paying customers or clients. Therefore, they are beneficiaries of the products and services offered by that business. At the same time, the general public may benefit in several ways such as a source of employment or by provision of infrastructure.

For example, university's customers include its students and faculty. Other beneficiaries include the immediate community such as lecturers and often the world population that enriched by results of research and service.

For varying degrees, these beneficiaries depend directly or indirectly on the existence of or access to computers, their data and programs, and their computational power. For these set of beneficiaries, continuity and integrity of computing are very important. In addition, beneficiaries' value confidentiality and correctness of the data involved. Thus, the interests of beneficiaries of a system must be reflected in the system's security policy.

7.1.2.3 Security Policy Contents

"Content Security Policy is intended to mitigate a large class of Web Application Vulnerabilities: Cross Site Scripting. Cross Site Request Forgery has also become a large scale problem in Web Application Security, though it is not a primary focus of Content Security Policy".

Figure 7.6: Examples of security goals

Based from the statement given, use the internet to clarify on the matter. Discuss your findings in the LMS Forum.

A security policy must identify its audiences which are the beneficiaries, users and owners. It also should describe the nature of each audience and their security goals. Several other sections are required is shown in Figure 7.6 followed by the description of each security goals.

1. Purpose

The policy should state the purpose of the organisation's security functions reflecting the requirements of beneficiaries, users and owners.

For example, the policy may state that the system will "protect customers' confidentiality and preserve a trust relationship", "ensure continual usability" or "maintain profitability".

The following Figure 7.7 displays examples of goals in security policy.

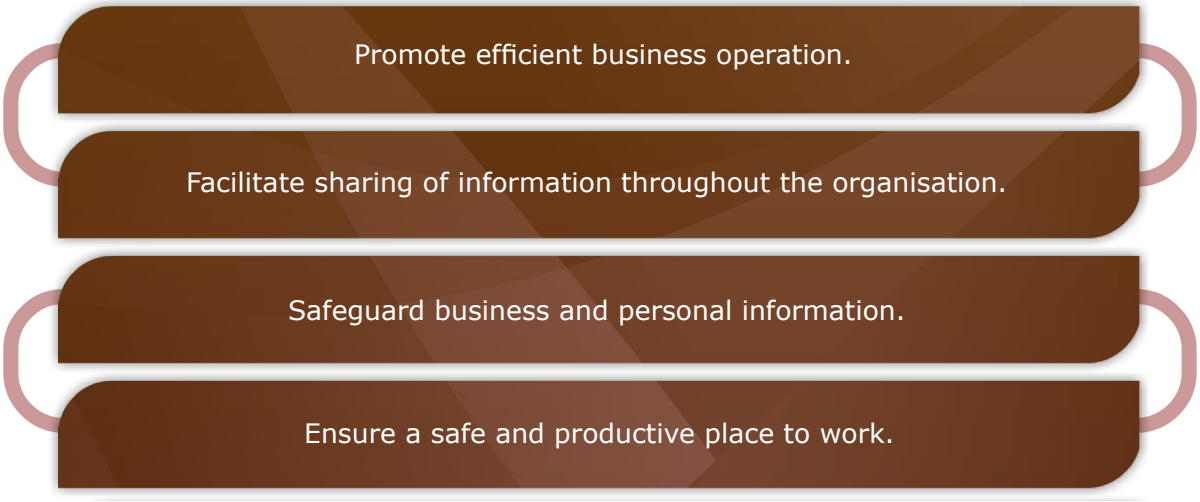


Figure 7.7: Examples of goals in security policy

The security goals should be related to the overall goal or nature of the organisation. It is important that the system's purpose to be stated clearly and completely because subsequent sections of the policy will relate back to these goals that making the policy a goal-driven product.

2. Protected Resources

A risk analysis will have identified the assets that are to be protected. These assets should be listed in the policy in the sense that the policy lays out which items it addresses.

The questions that can be helped to identify whether the assets should be protected are as shown in Figure 7.8.

Figure 7.8: Questions that can be helped to identify whether the assets should be protected

The policy also should state the difference if the degree of protection varies from one service, product or data type to another.

3. Nature of Protection

The asset list tells us what should be protected. The policy should also indicate who should have access to the protected items. It may also indicate how that access will be ensured and how unauthorised people will be denied access. Thus, the security policy should state what degree of protection should be provided to which kinds of resources.

7.1.2.4 Characteristics of a Good Security Policy

If security policy is written poorly, it cannot guide the developers and users in providing appropriate security mechanisms to protect important assets. Certain characteristics make a security policy is a good one. The characteristics are described in Table 7.2.

Table 7.2: Characteristics of a Good Security Policy

Characteristics	Descriptions
System Access Control	• A security policy must be comprehensive. • It must either apply to or explicitly exclude all possible situations. • Furthermore, a security policy may not be updated as each new situation arises, so it must be general enoughto apply naturally to new cases that occur as the system is used inunusual or unexpected ways.
Durability	• A security policy must grow and adapt well. In large measure, it will survive the system's growth and expansion without change. • If written in a flexible way, the existing policy will be applicable to new situations. • However, there are times when the policy must change such as when the government regulations mandate new security constraints, so the policy must be changeable when it needs to be. • An important key to durability is keeping the policy freefrom ties to specific data or protection mechanisms that almost certainly will change. • It is preferable to describe assets needing protection in terms of their function and characteristics rather than in terms of specific implementation.

Realism	• The policy must be realistic. • That is, it must be possible to implement the stated security requirements with existing technology. • Moreover, the implementation must be beneficial in terms of time, cost and convenience. • Thus, the policy should not recommend a control that worksbut prevents the system or its users from performing their activities and functions.
Usefulness	• An obscure or incomplete security policy will not be implemented properly. • The policy must be written in language that can be read, understood and followed by anyone who must implement it or is affected by it. • Therefore, the policy should be succinct, clear and direct.

7.1.3 Security Guidelines

Security guidelines assist in effectively securing the systems. The nature of guidelines however immediately recognises that systems vary considerably and imposition of standards is not always achievable, appropriate or cost-effective.

For example, an organisation guideline may be used to help develop system-specific standard procedures. Guidelines are often used to help ensure that the specific security measures are not overlooked although they can be implemented and correctly so in more than one way.

7.2 AWARENESS, ETHICAL AND EMPLOYMENT ENFORCEMENT

Data classification entails analysing the data of your organisation retains, determining its importance and value, and then assigning it to a category. The implementation and regimented use of a data classification program is a mark of a truly professional information security program. Data classification systems provide users with a way to stratify sensitive information and apply appropriate safeguards to data with varying levels sensitivity in a consistent manner.

7.2.1 Security Awareness

Security awareness is the process of making people understands the implications of security on their ability to perform their job. It includes the importance of security, the use of security measures and the process of reporting security violations.

A security awareness program is critical to any security design. All the people involved with information must understand the importance of security and what their part is in maintaining the security of the information that is entrusted to them. Increased awareness increases the proper use of security features and the likelihood that a user will report suspicious activities.

Employee education in security awareness can be a tremendous advantage to the organisation's security program. Employees who understand the value of security and how it affects them are more likely to utilise it.

There are a number of areas that need to be addressed in an awareness program as shown in Figure 7.9.

Figure 7.9: Questions regarding the areas that need to be addressed in an awareness program

Security awareness efforts are designed to change behavior or reinforce good security practices. Awareness is defined in NIST Special Publication 800-16 as follows:

> *"Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognise IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance."*

An example of a topic for an awareness session (or awareness material to be distributed) is virus protection. The subject can simply and briefly be addressed by describing what a virus is, what can happen if a virus infects a user's system, what the user should do to protect the system, and what the user should do if a virus is discovered.

Awareness and training programs must be designed with the organisation mission in mind. It is important that the awareness and training program supports the business needs of the organisation and be relevant to the organisation's culture and IT architecture. The most successful programs are those that users feel are relevant to the subject matter and issues presented.

7.2.1.1 Appropriate Use

Awareness and training program should be design by considering the following (see Figure 7.10).

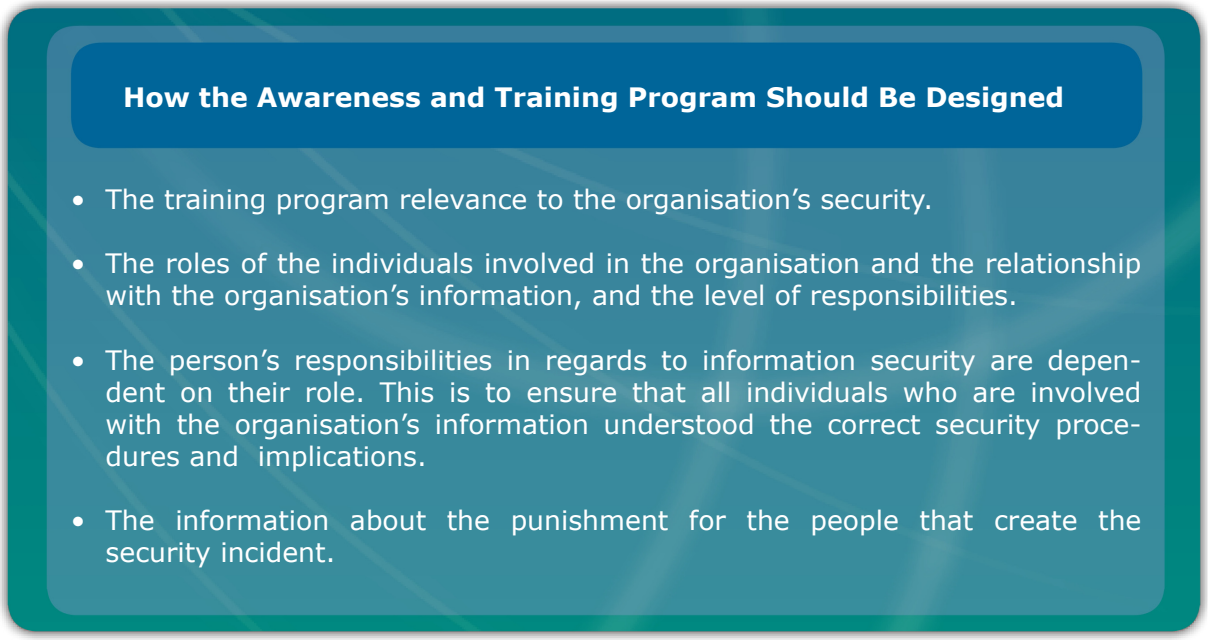


Figure 7.10: How the awareness and training program should be designed

7.2.1. 2 Awareness Program

Observe the video. Based from the video, highlight the keypoints mentioned.

Source: http://www.youtube.com/watch?v=FHcwQ4IplD4

Awareness program should start before an individual has access to company resource. It has to be made available to everyone in the organisation and those outside the organisation who will be granted access to information. It must keep the message fresh and in front of its audience so that it is not forgotten and it must be understood by everyone.

Awareness program must be continuous, comprehensive, coherent and cost effective. Continuous means that the program must support ongoing communication in which this program must have plenty opportunities to remind people that security is an ever-present concern. The security message can stand by itself or it can easily integrated into almost any business-related communication.

Comprehensive is referring to the content of the program should be covered all the importance of the information security. Thus, everyone in the organisation should understand on the importance of the information security and how to handle the information appropriately. The message from the awareness program must be understood.

It must be coherent where the message can be given in different styles or media such as written, visual, audio, humor stories or war stories, etc. The message needs to be brought into the real world with real world examples, analogies and actual events that put the issues into terms that are familiar to the individuals and can be easily absorbed.

In most organisations, security is viewed as a cost whose services are not used until after there is an incident, instead of a process that continuously reduces losses to an organisation by preventing incidents. Because of this, the cost of security program must be improved by having measurable results and the effectiveness of the an awareness program should be measured by reviewing and evaluating the feedback to identify whether everyone getting the message or not.

7.2.1.3 Awareness Implementation Options

The implementation of the awareness program can use several options such as (see Figure 7.11).

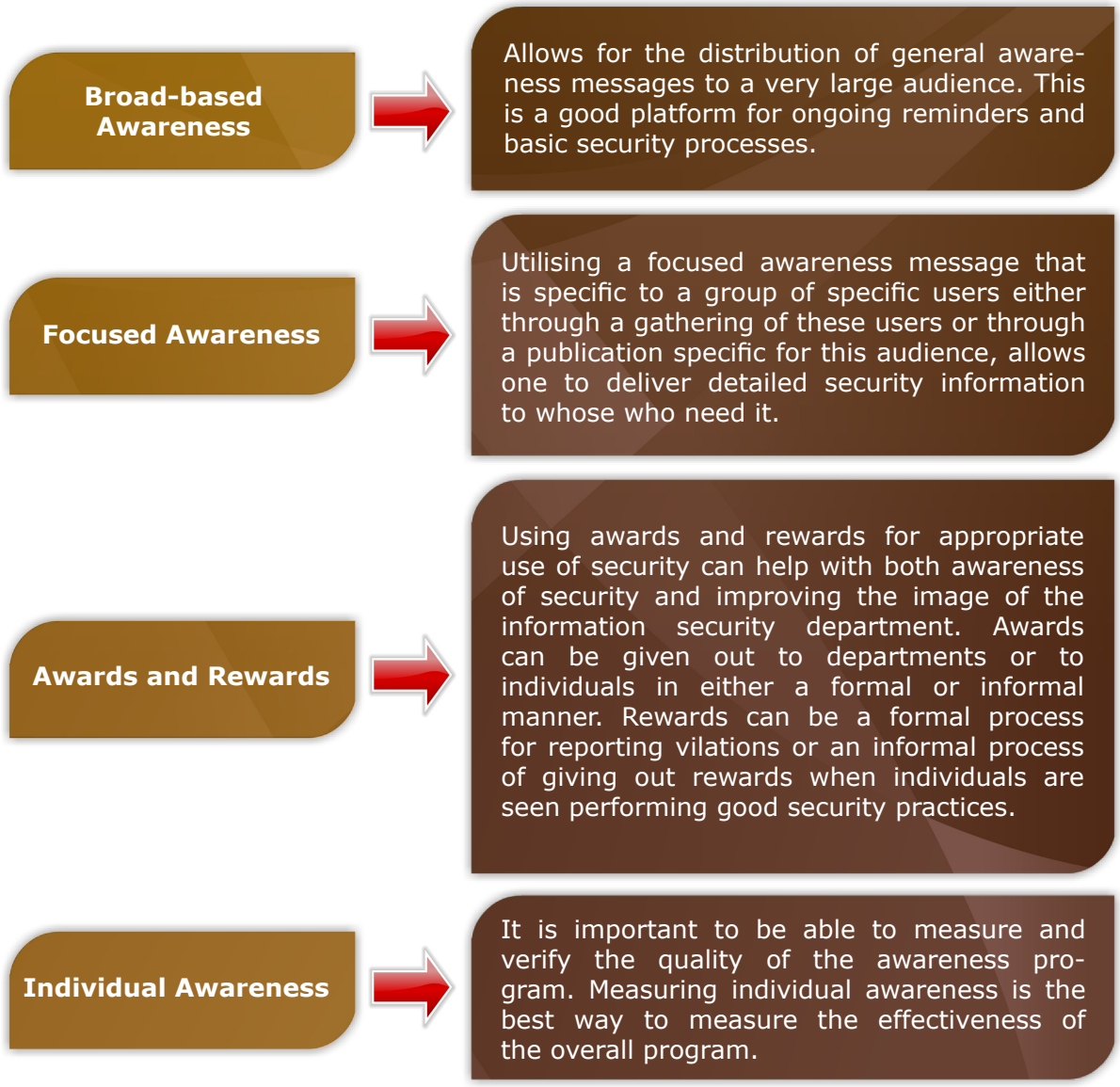


Figure 7.11: Awareness implementation options

7.2.1.4 Lack of Awareness

Lack of awareness can lead to a variety of security issues. The requirements of a security system often create more work for the users such as remembering and entering password. Users can be very creative in bypassing security features to make their life simpler. Without understanding the implications security features, the users may be unaware of the amount of time, effort and data can be lost by not using them.

7.2.2 Ethical Issues In Computer Security

There are a few differences between law, ethics and religion. Difficult choices would be easier to make if there were a set of universal ethical principles to which everyone agreed. However, the diversity of social, cultural and religious beliefs makes the identification of a set of universal principles impossible to which everyone agreed impossible.

Ethics and Religion

It is important to distinguish ethics from religion because ethical principles are different from religious beliefs. Two people with different religious backgrounds may develop the same ethical philosophy, while two exponents of the same religion might reach opposite ethical conclusions in a particular situation. We can also analyse a situation from an ethical perspective and reach ethical conclusions without appealing to any particular religion.

Ethics is Not Universal

Ethical values is not universal, it varies by society and within a society. For example, westerners and easterners have different view on privacy. The attitudes of people may be:

- Affected by culture or background.
- Influenced by past events in life.
- Affected by major events or close contacts with others.

However, the underlying principles of how to make moral judgement are the same.

Ethics Does Not Provide Answers

Ethical pluralism is recognising or admitting that more than one position may be ethically justifiable, even equally so, in a given situation. Pluralism is another way of noting that two people may legitimately disagree on issues of ethics.

This is different from scientific and technical fields where people expect to find unique,

unambiguous and unequivocal answers.

The basis of science is presumed to be 'truth'. A statement is expected to be provably true, provably false, or unproven but a statement can never be both true and false. Therefore, scientists are uncomfortable with ethics because it does not provide these distinctions.

Ethical Reasoning

Figure 7.12 represents the study in ethical reasoning.

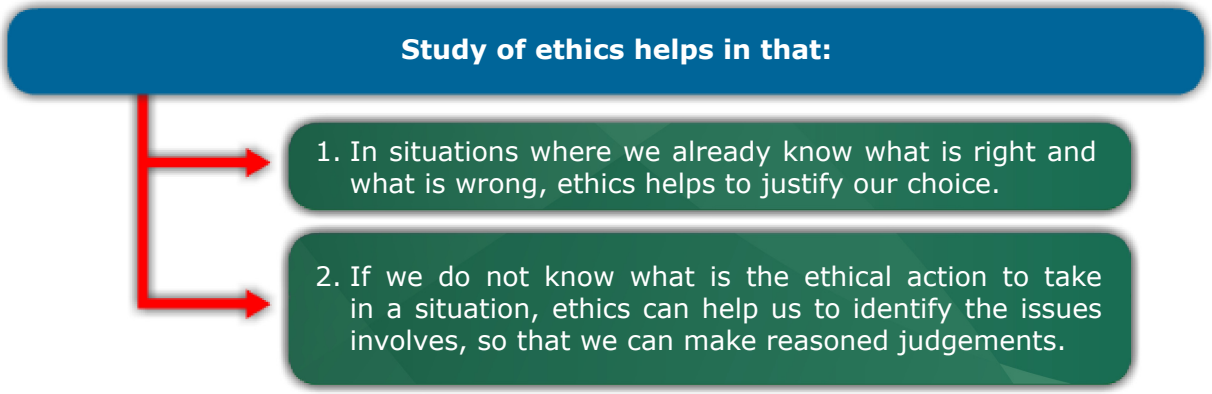
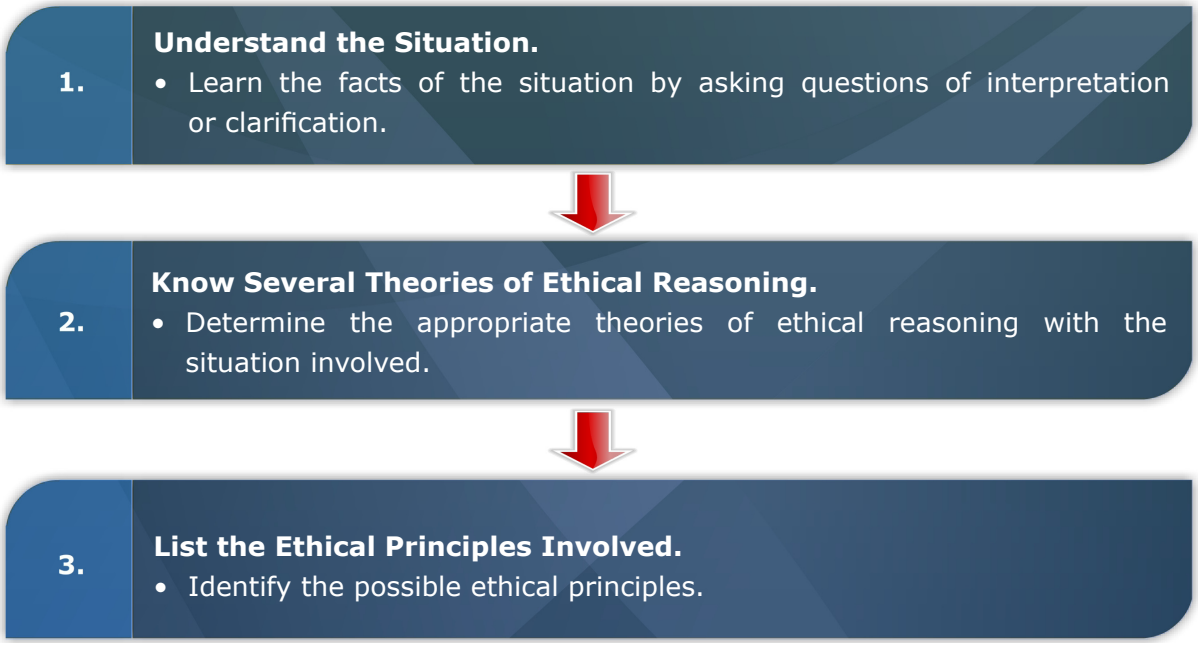


Figure 7.12: Ethical reasoning

7.2.2.1 Examining a Case for Ethical Issues

Figure 7.13 display the steps in making and justifying an ethical choice. In this steps involved, the most important steps are the first and the third.



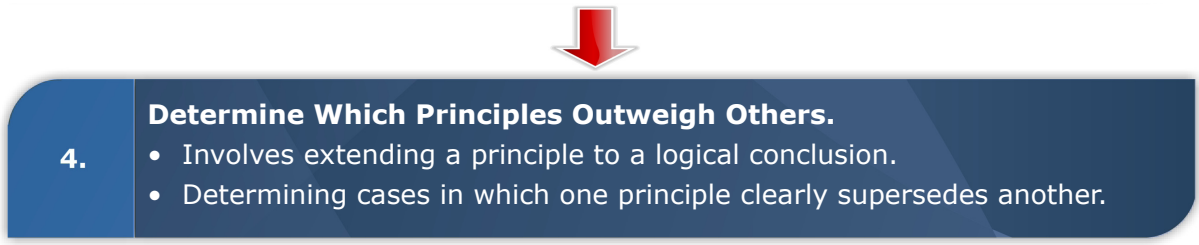


Figure 7.13: Ethical problem solving steps

7.2.2.2 Examples of Ethical Principles

There are two types of ethical principles in computer security. These types are shown in Figure 7.14.

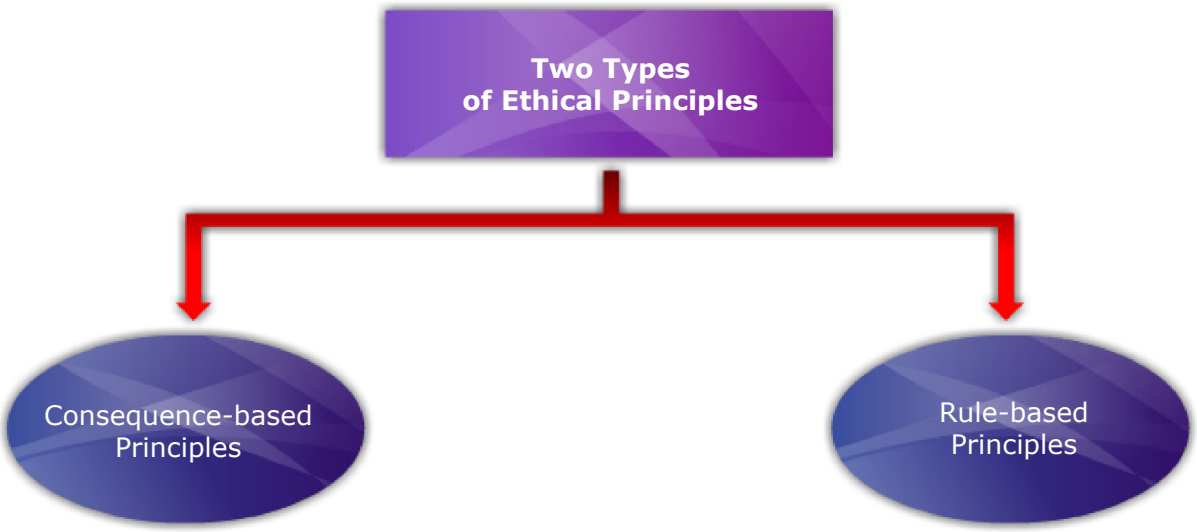


Figure 7.14: The two types of ethical principles in computer security

Now, from Figure 7.14, let us look into each of the ethical principles in details.

1. Consequence-Based Principles

This is the teleological theory of ethics. It focuses on the consequences of an action. The action to be chosen is that which results in the greatest future good and least harm. All theology theories of behavior focus on the goal, outcome or consequence of an action.

There are two forms of teleology:

(a) **Egoism** - the form that says a moral judgement is based on the positive benefits to the person taking the action. An egoist weighs the outcomes of all possible

acts and chooses the ones that produce the most personal good with the least negative consequence.

(b) **Utilitarianism** - an assessment of good and bad results, but the reference group is the entire universe. The utiliarian chooses that action that will bring the greatest collective good for all people with the least possible negative for all.

2. Rule-Based Principles

This is the deontological theory of ethics. This states that certain things are good in and of themselves. Examples of these intrinsic good things are:

- truth, knowledge and true opinion of various kinds, understanding, wisdom.
- just distribution of good, evil, justice.
- pleasure, satisfaction, happiness, life, consciousness.
- peace, security, freedom.
- good reputation, honor, esteem, friendship, cooperation.
- beauty, aesthetic experience.

With rule-deontology, one believes that there are certain universal, self-evident, natural rules that specify our conduct. Certain basic moral principles are adhered to because of our responsibilities to one another. These principles are often stated as rights.

As a conclusion, an ethical question is tackled by weighing values in terms of what a person believes to be right behavior.

7.2.3 Rights of Employees and Employers

Ownership is an issue of computer security because it relates to the rights of an employer to protect the secrecy and integrity of works produced by the employees. Protection offered by copyrights, patents and trade secrets applies to the ideas and products.

Ownership of Products

Ownership of product has many different situations. Because of this, the interpreting the laws of ownership is difficult. The following are several types of protections for several situations. Figure 7.15 displays examples ownership rights for employees and employers.

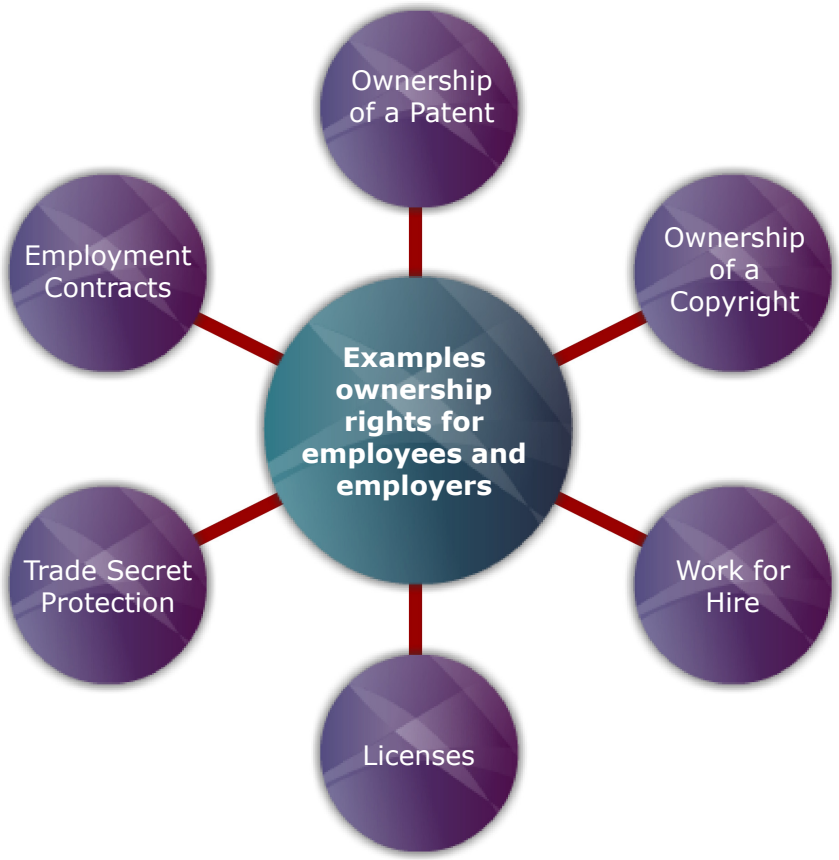


Figure 7.15: Examples ownership rights for employees and employers

1. Ownership of a Patent

The person who owns a work under patent or copyright law is the inventor. It is important to know who files the patent application. If an employer patent an invention, the employer, and not the employee who originated the idea, is deemed to own the patent and therefore the rights to the invention. The employer also has the right to patent if the employee's job functions included inventing the product. If an employee patents something, the employer can argue for a right to use the invention if the employer contributed some resources e.g. computer time in developing the invention.

2. Ownership of a Copyright

It is similar to ownership of a patent. The programmer is the presumed owner of the work. The owner has all rights to an object. A special situation known as work for hire applies to many copyrights for development of software of other products.

3. Work for Hire

In a work for hire situation, the employer is considered the author of a work, not the employee.

An employer may be in a work for hire relationship with an employee if the following conditions are true.

- The employer has a supervisory relationship overseeing the manner in which the creative work is done.
- The employer has the right to fire the employee.
- The employer arranges for the work to be done before the work was created (as opposed to the sale of an existing work).
- A written contract between the employer and employee states that the employer has hired the employee to do certain work.

No one of the above conditions is decisive. The more the conditions are true, the more a situation resembles work for hire.

4. Licenses

It is an alternative to 'work for hire' arrangement. The programmer develops and retains full ownership of the software. The programmer grants a license to a company to use the program. This license can be:

- For a definite or unlimited period of time;
- For a copy or unlimited copies;
- To be used at one location or many;
- To be used on a machine or all machines; and
- To be used at specified or unlimited times.

5. Trade Secret Protection

A trade secret is not registered. However, the ownership must be established. The company which owns the trade secrets treats the information as confidential data. As soon as a secret is developed, the company becomes the owner. As with copyrights, an employer may argue about having contributed to the development of trade secrets.

6. Employment Contracts

Commonly an employment contract will express the rights of ownership. It is desirable, so that both parties (the employees and employers) will understand their rights and responsibilities.

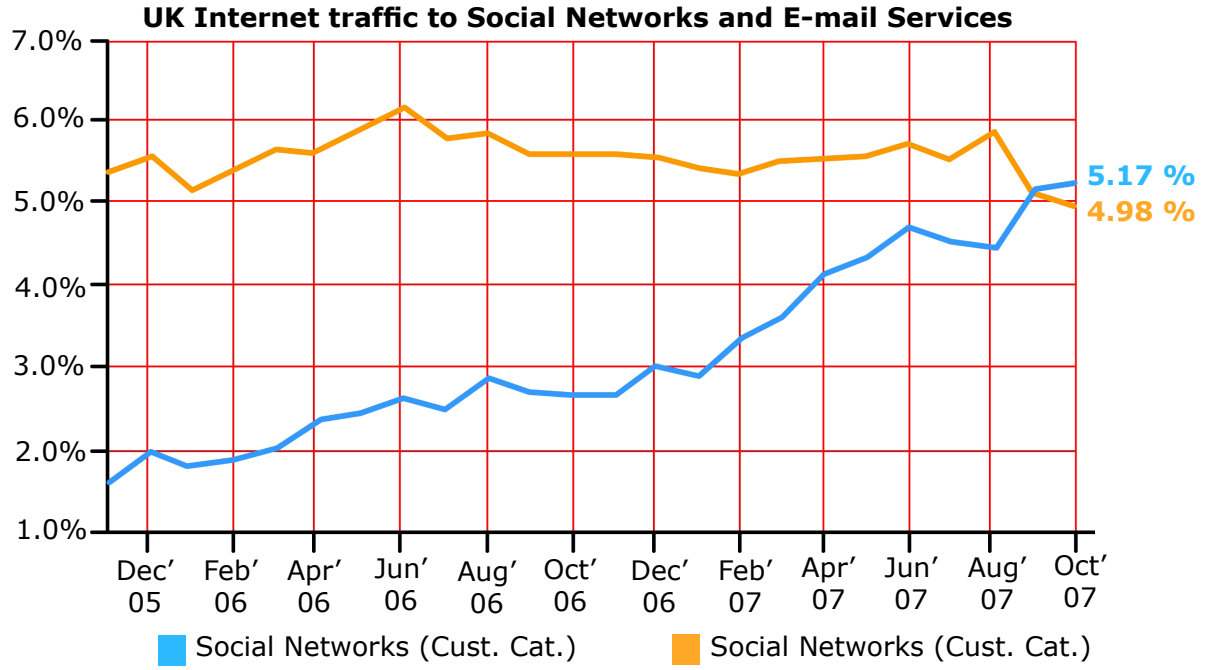
- Typically an employment contract specifies:;
- The employee is hired to work as a programmer exclusively for the benefit of the company;
- The company states that it is a work for hire situation;
- The company claims all rights to any programs developed, including all copyright rights and the right to market;
- The employee receives access to certain trade secrets as a part of employment, and

the employee agrees not to reveal those secrets; and

- Sometimes an agreement not to compete is included, i.e. the employee is not to compete by working in the same field for a set period of time after termination.

7.3 E-MAIL AND INTERNET USAGE

Look at the chart below.



Source: http://www.saasology.net/2007/12/social-networks.html

The chart displays the UK Internet traffic for internet and e-mail usage. Based from the chart above, identify the factors for the overtook in usage of the internet and e-mails.

The widespread use of the Internet and electronic mail ("e-mail") has transformed the way business is conducted in the typical American workplace. Written communication to almost anyone in the world now can be completed nearly instantaneously; information about any subject encountered in a daily job task can be retrieved in seconds from the Internet through multiple search engines. These technological developments have benefited employers and employees alike employers in accomplishing business goals and employees in performing their duties. Undoubtedly, the Internet and e-mail also have given employees a new means of escaping briefly from long days at the office.

An employee's personal use of an employer's e-mail system and of Internet access is not protected under the law, and employers can face legal liability for employees' inappropriate use thereof. Therefore, all the organisations and companies have their own email and internet policy.

Both employers and employees agree that non-work-related use of the Internet and e-mail is appropriate, and indeed, many employees now see such activity as essential to "making it through" the workday.

As with most things in life, a commonsense approach to this issue minimises the risks for all involved: employees must acknowledge that their employers can and will monitor their use of these two electronic means of communication to ensure that it is not excessive, inappropriate, or illegal, and employers must make all employees aware of their policies and procedures with respect to the Internet and e-mail, review employee activity or quickly taking remedial action when those policies or procedures are violated.

7.3.1 Internet Usage

The Internet policy is to provide guidance for acceptable use for Internet to the organisation's employees. The purpose of providing access to the Internet is to support the business activities by the organisation employees and related agencies. The Internet will provide employees with a fast and convenient resource for the exchange of information.

The equipment necessary to access the Internet is the exclusive property of the organisation, and therefore any access is to be used for official business purposes only. Access to the Internet will be at the sole discretion of management.

The organisation will actively monitor use of the Internet, to ensure that anyone using the organisation access to the Internet does not engage in any unethical, illegal or unacceptable activity.

Examples of unethical, illegal or unacceptable activities include, but are not limited to:

- Seeking to gain or gaining unauthorised access to information resources.
- Gaining, communicating, or using passwords belonging to other users.
- Using the Internet to access, process, distribute, transmit or display inappropriate stored electronic media; obscene, libelous or defamatory material, or any material, the access to which might undermine the integrity of the organisation.
- Participating in "chat rooms".
- Submitting, publishing or displaying any defamatory or obscene material, either public or private.
- Using the Internet for personal gain or profit.

- The use of "Web Radio", "Web Shots", "Weather Bug", "Napster" (or the equivalent), "Web Casts", "Web Robots" or any other real-time connections which occupies continuous bandwidth (resources) in the network.

If an employee is found to have engaged in any unethical, illegal or unacceptable activities, such activity will subject the user to discipline consistent with any applicable labor agreement or policy including revocation of rights to Internet access.

In order to maintain network security and comply with the Country Services Agreement for Internet Access Services, all employees using the organisation access to the Internet are expected to comply with the following:

- All files downloaded from the Internet must be scanned with anti-virus software approved by administrator or services.
- No computer used for Internet access can be running peer-to-peer network services.
- No computer used for Internet access can be connected to another Internet service.
- Provider other than what is provided by the organisation.
- Any employee that feels he or she can identify a security concern or feels that his or her system may be infected with a computer virus should perform no further work on the computer and immediately contact the administrator in charged.

7.3.2 E-mail Usage

The email policy is to provide guidance for acceptable use for email to the organisation's employees. Any computer or LAN/WAN Network resource provided for use by the organization employees, contractors and consultants is the organisation property and all uses of these organisation resources are a matter of organisation record. Therefore, they are subject to internal and/or external review, auditing, and recall as provided by law.

The e-mail function, like any organisation resource, must be used for official business only. Towards the end, the organisation reserves the right to designate person(s), position(s), and/or committee(s) which have authority to monitor all electronic mail systems and mail distribution resources to ensure that the e-mail system is being used for its intended purpose.

The monitoring will be confidential, and limited to a review of traffic log files. In addition, at the request of the organisation elected officials or department heads, County Management and Technology Services Department have the rights to review the contents of employees' e-mail communications when there is a reasonable, articulable suspicion that the function is being misused.

7.4 AUDIT AND CONTROL

Security audit and security control is very important to ensure that the organisation is not under risk situation. It might help the organisation to prevent their system from any possible threats.

7.4.1 Security Control

The basic responsibility of an information security practitioner is to maintain security control of the networks and systems under his or her authority. Therefore, administrators are responsible for ensuring that their security mechanisms enforce three basic requirements that are (see Figure 7.16).

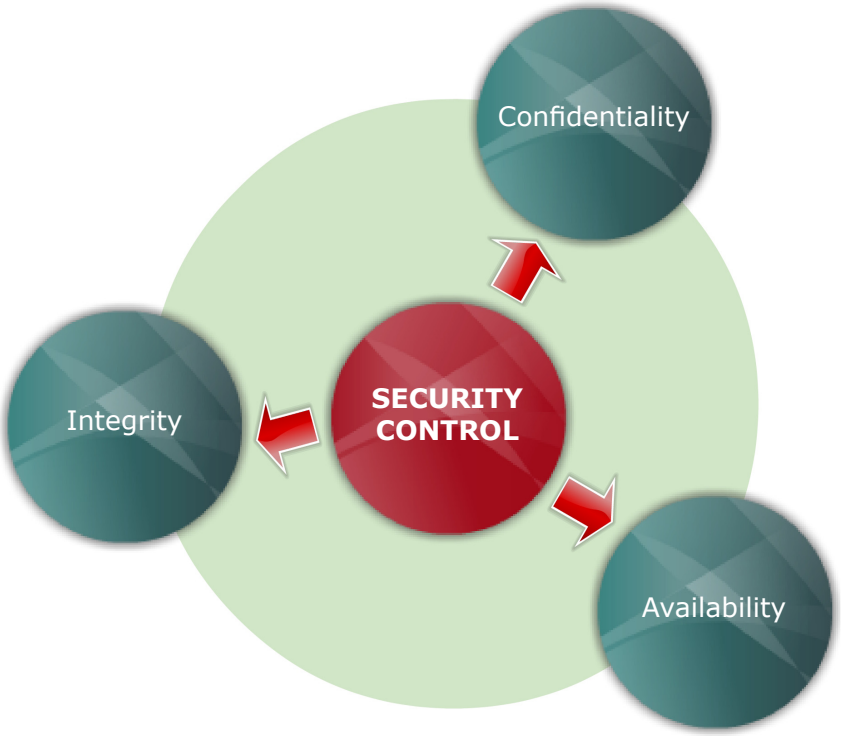


Figure 7.16: The three types of security control

These fundamental building blocks of information security are interdependent. If one of these elements is violated, you lose security control of the system or network in question.

Confidentiality: All data on the secured system or networks must be protected from unauthorised disclosure. Measures must be in place to prevent unauthorised individuals from accessing information either by outsiders gaining illegitimate access to the system or insiders exceeding their legitimate authority.

Integrity: All data on the secured system or network must be protected against unauthorised modification. If an attacker manages to modify sensitive data without being detected, the consequences could be worse than if the data was merely disclosed to an unauthorised individual as organisation insiders may then unsuspectingly act upon this erroneous information.

Availability: The systems themselves must be protected in such a manner as they are available to authorised users during their normal operating hours. If an attacker is able to successfully deny an authorised user access to critical information, the attack may be just as successful as if he or she were able to steal or modify that same information.

7.4.1 .1 Security Control Characteristics

The information security control has two major characteristics as shown in Table 7.3.

Table 7.3: The Two Major Characteristics of Security Control

Information security control characteristics	Descriptions
Dynamic	• Information system is a dynamic system which needs its security characteristic to change auto-adapted along with the dynamic change. • Often there are one or several safety zones in information system, each of which has its own special rules, such as forbidding all accesses and so on. • The users' privilege will never allow them to access the region. When the safety zone area extends or reduces, user's jurisdiction is going to change along with it. • For example the corresponding jurisdiction will be automatically deleted if the area extends. • From it we can see that user's jurisdiction and the safety zone is always dynamical equilibrium, the more one becomes the less the other becomes, vice versa.
Bi-direction	• The information flowing of information system is bidirectional which includes not only threat from exterior to interior but also threat from interior to exterior. • Since there are various safe threats in the system we must take some measures to protect the information. • First of all it is to block all known dangerous sources from exterior systems in advance; besides it we need to establish

a perfect mechanism of safety control to prevent it from attacking the exterior system.

- Concretely, we could build a safety control strategy database for some special information system to minimise the threat so as to keep the system in safe.

7.4.1.2 Security Control Model

In the model of the information security control as shown in Figure 7.17, the information input carries on the safe operation after the security decision-making, thus achieves a certain secure state. After evaluating the security state and the security goal, the new safe request feeds back to the place of initial information input, starts new turn iteration and then achieves the final security goal.

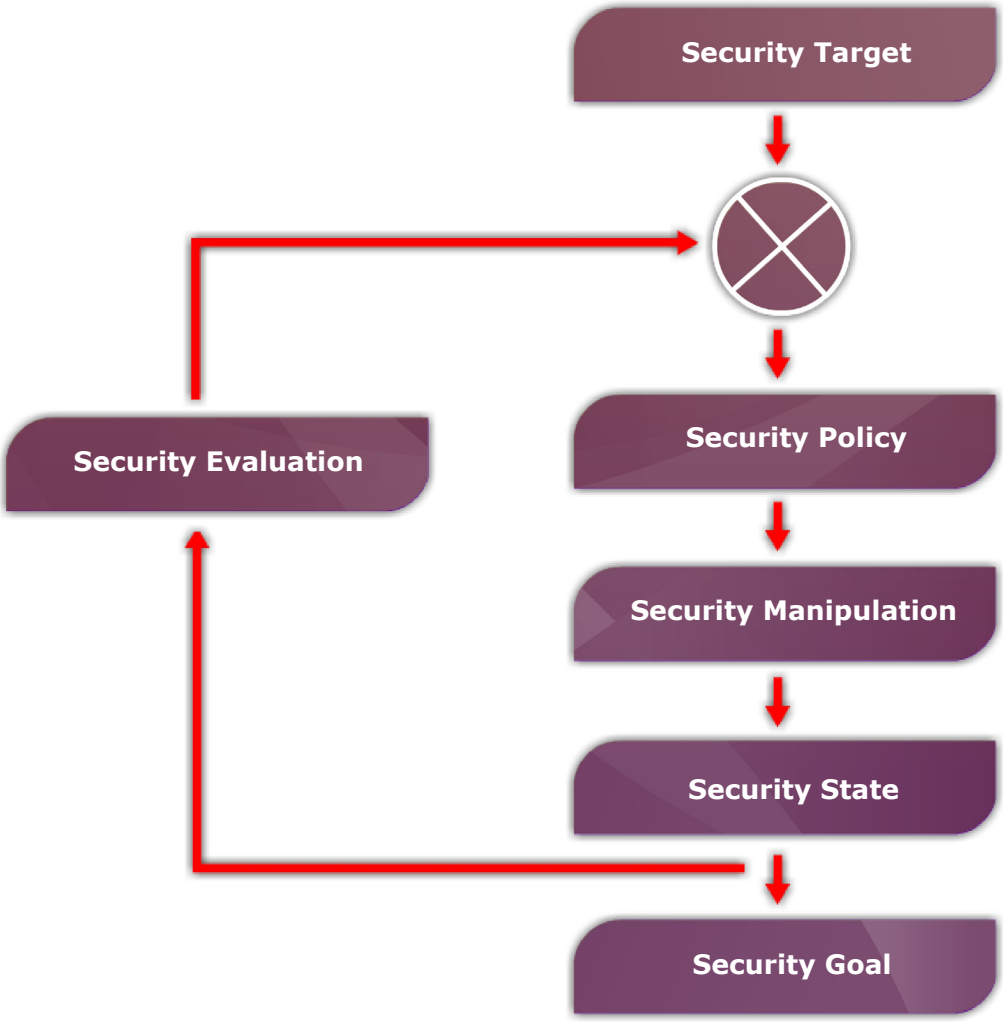


Figure 7.17: Security Control Model

7.4.1.3 Security Control System

The information security control system consists of authentication and authorisation, monitoring system, control system and authorised operation. The nature of dynamic and bi-direction are the main characteristics of information security control system. The automatic control system assumes the responsibility of the dynamic update of the information system's security state. As for the safe threat from inside and outside, the security control will monitor the bidirectional information flows to assure that those legitimate and illegal information flows would be forbidden. That is how the information security controls to secure the system.

7.4.2 Security Audit

A security audit is a systematic, measurable technical assessment of how the organisation's security policy is employed at a specific site. It is a manual or systematic measurable technical assessment of a system or application (see Figure 7.18).

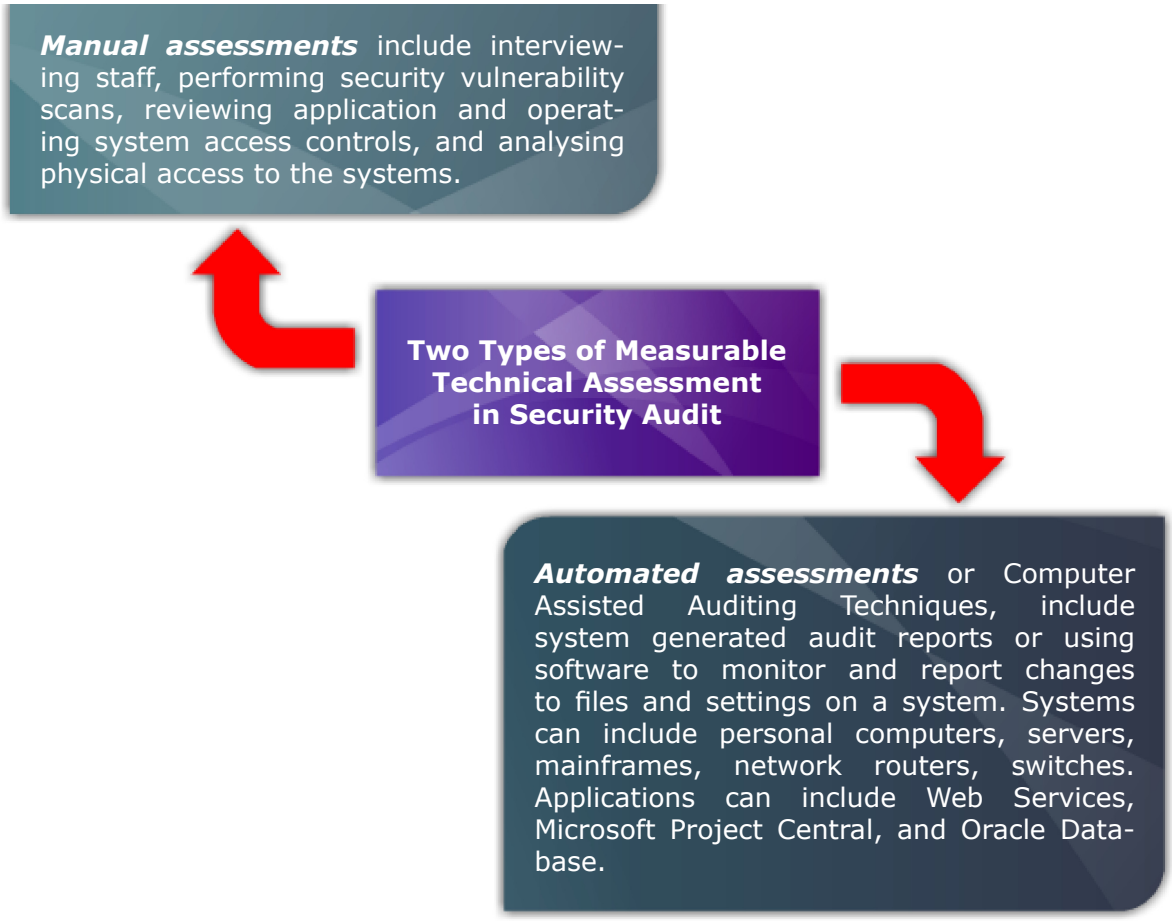


Figure 7.18: The two types of measurable technical assessment in security audit

Security audit is different with penetrating testing because a penetration test is a very narrowly focused attempt to look for security holes in a critical resource, often with little or no "inside" knowledge and usually conducted outside the firewall. On the other hand, Computer security auditors work with the full knowledge of the organisation, often with considerable inside information, in order to understand the resources to be audited.

Security policies help standardise security practices by having them codified (in writing) and honored by employees who agree to follow these practices. The security policy lists acceptable practices for everyone to follow as they perform their daily tasks. They are based on "Industry Best Practices". The unwritten security policy is the actual way security is implemented in an organisation. It relies on workplace customs.

Because it's unwritten, it isn't always understood by everyone. Therefore, security audits have to be able to gauge both the written and unwritten security policies. Auditors therefore rely on many methods to get a clear picture of an organisation.

7.4.2.1 Security Audit Standard

There are a number of IT security standards. These standards represent the best security practices of a particular work sector and are tailored for that sector. Security audit standards are checklists examining specific procedures that should be followed to ensure that IT resources are adequately safeguarded.

Examples of IT Security Audit Standard are shown in Figure 7.19.

Figure 7.19: Examples of IT Security Audit Standard

7.4.2.2 Security Audit Methods

A security audit consists of several processes which are divided into four stages. These stages are described in Figure 7.20.

Figure 7.20: The four stages in security audit methods

1. Audit planning and preparation

In preparing for an audit, auditors consult previous audit results, site surveys, and questionnaires. In addition, they consult with the client in order to limit the scope of the audit. The auditor should be adequately educated about the company and its critical business activities before conducting a data center review. The objective of the data center is to align data center activities with the goals of the business while maintaining the security and integrity of critical information and processes.

To adequately determine if whether or not the client's goal is being achieved, the auditor should perform the following before conducting the review:

- Meet with IT management to determine possible areas of concern.
- Review the current IT organisation chart.
- Review job descriptions of data center employees.
- Research all operating systems, software applications and data center equipment operating within the data center.
- Review the company's IT policies and procedures.
- Evaluate the company's IT budget and systems planning documentation.
- Review the data center's disaster recovery plan.

All information above can be obtained using site surveys method which site surveys are provided by the client. They are technical descriptions of the network resources to be audited. They lists computers, operating systems and have network diagrams.

2. Establishing audit objectives

The next step in conducting a review of a corporate data center takes place when the auditor outlines the data center audit objectives. The computer security audit is conducted in stages with a fair amount of coordination between client and auditor. The audit consists of an arrival briefing, data collection and departure briefing. Auditors consider multiple factors that relate to data center procedures and activities that potentially identify audit risks in the operating environment and assess the controls in place that mitigate those risks. After thorough testing and analysis, the auditor is able to adequately determine if the data center maintains proper controls and is operating efficiently and effectively.

Following is a list of objectives the auditor should review:

- Personnel procedures and responsibilities including systems and cross-functional training.
- Change management processes are in place and followed by IT and management personnel.
- Appropriate back up procedures are in place to minimize downtime and prevent loss of important data.
- The data center has adequate physical security controls to prevent unauthorised

access to the data center.

- Adequate environmental controls are in place to ensure equipment is protected from fire and flooding.

3. Performing the review

The next step is collecting evidence to satisfy data center audit objectives. This involves traveling to the data center location and observing processes and procedures performed within the data center. The following review procedures should be conducted to satisfy the pre-determined audit objectives as shown in Table 7.4.

Table 7.4: The Pre-determined Audit Objectives

Audit objectives	Explanation
Data center personnel	• All data center personnel should be authorised to access the data center (key cards, login ID's, secure passwords, etc.). • Data center employees are adequately educated about data center equipment and properly perform their jobs. • Vendor service personnel are supervised when doing work on data center equipment. • The auditor should observe and interview data center employees to satisfy their objectives.
Equipment	• The auditor should verify that all data center equipment is working properly and effectively. • Equipment utilisation reports, equipment inspection for damage and functionality, system downtime records and equipment performance measurements all help the auditor determine the state of data center equipment. • Additionally, the auditor should interview employees to determine if preventative maintenance policies are in place and performed.
Policies and Procedure	• All data center policies and procedures should be documented and located at the data center. • Important documented procedures include: - Data center personnel job responsibilities; - Back up policies, security policies;

	- Employee termination policies; - System operating procedures; and - An overview of operating systems.
Physical security/ environmental controls	• The auditor should assess the security of the client's data center. Physical security includes bodyguards, locked cages, man traps, single entrances, bolted down equipment and computer monitoring systems. • Additionally, environmental controls should be in place to ensure the security of data center equipment. These include: Air conditioning units, raised floors, humidifiers and uninterruptible power supply.
Backup procedures	• The auditor should verify that the client has backup procedures in place in the case of system failure. • Clients may maintain a backup data center at a separate location that allows them to instantaneously continue operations in the instance of system failure.

4. Issuing the review report

The data center review report should summarise the auditor's findings and be similar in format to a standard review report. The review report should be dated as of the completion of the auditor's inquiry and procedures. It should state what the review entailed and explain that a review provides only "limited assurance" to third parties.

SUMMARY

1. It is very important to ensure that the organisation is secured.
2. Therefore, everyone should aware all the possible threats to their organisation and apply the law and ethic in the appropriate manner.
3. Everyone has to follow all the policies and standards that are provided by the organisation and play their role in the success of a security awareness and training program.
4. An organisation's information security policy should describe the measures taken within the organisation to protect the confidentiality, integrity and availability of data.
5. It should be developed using a multidisciplinary approach and maintained over time.
6. Audits are used to examine an organisation's security policy.
7. The security policy is both written and unwritten. Auditors have to consider both.
8. The audit is less about tools and checklists and more about identifying good and bad security practices in a fair and concise manner.

GLOSSARY

Auditing	The formal examination and review of actions taken by system users.
Policy	High-level statements made by management laying out the organisation's position on some issue.
Sarbanes-Oxley Act	Congressional law designed to combat issues of corporate governance and responsibility.
Security Control	Maintaining the confidentiality, integrity and availability of protected systems and networks.

Security Policy	Written documents that outline an organisation's security requirements and expectation of users, administrators, security professional and managers.
Standard	Accepted specifications providing specific details on how a policy is to be enforced.

DISCUSSION QUESTION

1. What is the difference between law and ethics in computer security?
2. Briefly discuss the characteristics for a good security policy.
3. What are areas that covered in ISO 17799 Standard?
4. Explain the process on conducting the security audit.
5. In this case, you will learn about ethical values that should involve in solving the daily problems whether at your home, workplace or anywhere. Upon completion this exercise, you should be able to analyse the situation involve, solve the ethical dilemmas as computer professional and determine ethical control and legal decision-making.

   Case: Rights of Employee and Employers (Release of software that may contain serious bugs)

   A small software company is working on an integrated inventory control system for a very large national computer manufacturer. The system will gather sales information daily from computer stores nationwide. This information will be used by the accounting, shipping and ordering departments to control all the functions of this large corporation. The inventory functions are critical to the smooth operation of this system.

   Zikriamri is the quality assurance engineer with the software company. He suspects that the inventory functions of the system are not sufficiently tested, although they have passed all the tests specified in the contract by the contractor. He is being pressured by his employers and fellow employees to sign off on the software.

   Legally, he is only required to perform those tests which had been agreed to in the original contract. However, her considerable experience in software testing has led him to be concerned over risks of the system. His employers say that will go out of business if they do not deliver the software on time.

His employers could fire him if he refuses to sign. But Zikriamri contends if the inventory subsystem fails, it will significantly harm their client and its employees. Now, Zikriamri is faced by a difficult moral decision. Is Zikriamri should release the software?

Imagine you are in Zikriamri shoes, what is your decision? In making your decision, consider the following issues:

- The ethical principles/values issues involve in this case.
- The legal issues involve in this case.
- The employee (Zikriamri) rights.
- The employer rights.

Use a word processor to write an analysis on making the decision. Identify whether it is an ethical decision or legal decision or both of it or partially. State your reasons based on your analysis done on issues involve in this case.

REFERENCES

Anonymous (2000). *Information Technology Security Standards*. Washington State Department of Information Services, Draft IT Security Guideline 6-22-00, http://isb.wa.gov/policies/portfolio/401S.doc [cited 5/4/09].

Anonymous (2009). *Information Security Audit*. http://en.wikipedia.org/wiki/Auditing_information_security [cited 5/4/09].

Anonymous. *ISO 17799 made easy*. http://17799.macassistant.com/def.htm [cited 5/4/09].

Bill Hayes (2002). *Computer Security Auditing*. www.certconf.org/presentations/2004/Wednesday/WA4.pdf [cited 5/4/09].

Charles P. Pleeger (2003). *Security in Computing*. New Jersey, United States: Prentice Hall.

Michael G. Solomon & Mike Chapple (2005). *Information Security Illuminated*. Sudbury, Massachusetts: Jones and Bartlett Publishers.

Siti Rahayu Selamat, Robiah Yusof, Mohd Faizal Abdollah & Nazrulazhar Bahaman, (2006). *Information Technology Security*. Malaysia: Prentice Hall.

Yuan Jia-bin & Gu Kai-kai (2007). I*nformation Security Control in the Application of Grid Security*. In the Proceeding of ATIP 3rd China HPC Workshop, ACM.