IT1105 – Information Systems and Technologies

BIT – 1ST YEAR – SEMESTER 1
University of Colombo School of Computing

Student Manual

Lesson 7:

Security, Privacy and Ethical Issues

By Yamaya Ekanayaka

Duration: 10 hrs

Instructional Objectives
Students will be able to:

- Describe some examples of waste and mistakes in an IS environment, their causes, and possible solutions
- Describe the types and effects of computer crime
- Discuss the principles and limits of an individual's right to privacy
- Identify ethical dimensions and important ethical issues associated with the use of computers
- Identify types of security management strategies and defences and describe how they can be used to ensure the security of business applications of IT
- Describe ethical responsibilities of IT Managers and users in the work environment

7 Security, Privacy and Ethical Issues

7.1 Computer Related Waste, Mistakes

7.1.1 Computer Related Waste and Mistakes

Computer technologies (software/hardware) change rapidly and sometimes organizations have to discard existing systems even if they are in the working condition. Discarded technology is one of the major computer wastes. In most of the organizations, majority of computers are in the standby mode , hence the processing power of the computer systems is not fully utilized. Thus, unused computers have become another type of computer waste in an organization. Since the introduction of the Internet and e-mail, personal use of corporate time and computer technology became the other type of computer waste.

An organization loses considerable amount of resources due to computer mistakes. These mistakes can be data entry or capture errors, programming errors/bugs, file management errors, insufficient disaster recovery plan etc.

7.1.2 Preventing Computer Related Waste and Mistakes

In order to overcome these computer wastes and mistakes, an organization should implement preventive policies and procedures that describe:

- Computer acquisition & use
- Individual and work group training
- Maintenance and use of computer systems
- Approval for applications & systems

Refer the main reference.

7.2 Privacy

Privacy can mean many things from the right to be left alone to the right to have some control over how your personal or health information is properly collected, stored, used or released.

We often think about privacy in different ways, for example:

physical privacy - such as bag searching, use of DNA

information privacy – the way in which government agencies or organizations handle personal information such as age, address, physical or mental health records

freedom from excessive surveillance – the right to go about our daily lives without being surveilled or have all our actions caught on camera.

7.2.1 Privacy Issues

One of the earliest computer ethics topics to arouse public interest was privacy. The ease and efficiency with which computers and computer networks can be used to gather, store, search, compare, retrieve and share personal information make computer technology especially threatening to anyone who wishes to keep various kinds of "sensitive" information (e.g., medical records) out of the public domain or out of the hands of those who are perceived as potential threats. During the past decade, commercialization and rapid growth of the Internet; the rise of the world-wide-web; increasing "user-friendliness" and processing power of computers; and decreasing costs of computer technology have led to new privacy issues, such as data-mining, data matching, recording of "click trails" on the web, and so on.

The variety of privacy-related issues generated by computer technology has led to re-examine the concept of privacy itself. Since the mid-1960s, for example, a number of scholars have elaborated a theory of privacy defined as "control over personal information".

7.2.2 Internet Privacy, Laws and Regulations

Internet privacy issues encompass concerns about the collection of personally identifiable information from visitors to government/commercial Web sites. Internet privacy issues also encompass concerns about debate over law enforcement or employer monitoring of electronic mail and Web usage. One aspect of the Internet privacy debate focuses on whether industry self regulation or legislation is the best route to assure consumer privacy protection. In particular, consumers appear concerned about the extent to which Web site operators collect "personally identifiable information" and share that data with third parties without their knowledge. Repeated media stories about privacy violations by Web site operators have kept the issue in the forefront of public debate about the Internet privacy.

In addition to the adult privacy, advocates have to focus on protecting the privacy of children as they visit commercial Web sites. Not only are there concerns about information children might divulge about themselves, but also about their parents. The Children's Online Privacy Protection Act (COPPA) in US addresses these issues but there are no such acts in the most of the countries.

Regarding the Internet privacy, privacy advocates are particularly concerned about online profiling, where companies collect data about what Web sites visited by a particular user and develop profiles of that user's preferences and interests for targeted advertising. Another concern is the extent to which electronic mail (e-mail) exchanges or visits to Web sites may be monitored by law enforcement agencies or employers. In the wake of the September 11 terrorist attacks in US, the debate over law enforcement monitoring has intensified.

7.2.3 Fairness in Information Use

In principle, there are four fair information practices. They are:

1. providing notice to users of their information practices before collecting personal information,
2. allowing users choice as to whether and how personal information is used,
3. allowing users access to data collected and the ability to contest its accuracy, and
4. ensuring security of the information from unauthorized use.

7.3 Security Threats/Computer Crime

At present, most of the organizations report computer crimes at an alarming rate. These crimes may be related to different types of security problems such as hacking, viruses, Trojan horses, worms, spyware, etc.

Most organizations have been victims of computer crime: When considered in light of the fact that many, if not most computer crimes go undetected, it is clear that the issue of security breaches should be of concern to every organization.

Computer crime causes significant damage: Not all organizations that were victimized by computer security breaches were able to quantify their losses. Notably, the theft of proprietary information resulted in the highest financial losses, continuing a rising trend, followed by financial fraud.

Computer crime is increasing: The problem of information security is not limited to the western countries; in fact, many of the crimes reported in the research originated outside the United States and Europe.

There are many costs associated with computer crime such as direct financial loss, loss of sales and privacy violation. Some of these costs are described below:

Direct financial loss: Customers' credit card numbers, the company's merchant account passwords, and employees' personal account numbers are all prime targets for thieves. Whether or not the criminal is brought to justice, indirect legal fees or fines resulting from the crime can add significantly to the costs, especially in industries like banking and finance.

Lost sales and reduced competitive advantage: When proprietary sales proposals, business plans, product designs or other information are stolen, altered or destroyed, it can give competitors a distinct advantage. Lost sales can result, and the impact can be felt long after the incident occurs.

Damage to your corporate reputation and brand: A company work hard to build and maintain their corporate image and to establish trusted relationships with their customers and business partners. If proprietary or private information is compromised, corporate credibility and business relationships can be severely damaged.

Privacy violation: Employees trust a company to keep their personal information private. Similarly, customers trust the company to keep their credit card numbers and credit histories confidential. If that privacy is violated, legal and other consequences can result.

Business disruption: When a service disruption occurs, a company's IT staff needs to address the problem immediately. They will be able to restore data from backup files, and return systems to service without significant downtime. However, in the case of mission critical systems such as air line reservation system, any downtime can be catastrophic.

Let's consider the security threats in the following sub-section.

7.3.1 Malicious Software

Malicious software, is also known as malware. This type of software is used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software. Malware includes computer viruses, worms, trojan horses, spyware etc.

A virus is a computer program that can spread across computers and networks by making copies of itself without the user's knowledge. Viruses can have harmful effects. For example they can steal confidential data, use your computer to attack web sites, corrupt data, delete data, damage user credibility and even disable and damage hardware devices. A virus program has to be run before it can infect a computer. Viruses have ways of making sure that this happens. A virus can be attached to an e-mail, document or a program. Then, the virus can copy itself to other files or disks and make changes on a computer. Virus can spread when we share electronic documents with other users using floppy disks, CDs or flash disks. Security vulnerability in an operating system or software also can allow viruses to infect the computer via the Internet. Email can include virus infected attachments. Some emails even include malicious virus scripts that run as soon as you preview the email.

Worms are similar to viruses but do not need a carrier program or document. Worms simply create exact copies of themselves and use a network to spread.

Trojan horses are programs that pretend to be legitimate software, but actually carry out hidden, harmful functions. Trojans cannot spread as fast as viruses because they do not make copies of themselves.

Spyware includes methods to collect information about the use of the computer on which the software is installed. When the computer is connected to the Internet, the spyware periodically relays the information back to the software manufacturer or a marketing company thus it clearly violate the user privacy. There are some spyware software that can record a person's keystrokes. All typed information thus can be obtained by another party, even if the author modifies or deletes what was written, or if the characters do not appear on the monitor (such as when entering a password).

7.3.2 Hacking and Cyber vandalism

Hacking refers to illegal access and abuse of computer resources. Security vulnerability in an operating system or computer software allows hackers to gain illegal access.

Cyber vandalism is a form of vandalism caused using a computer, and against electronic information.

7.3.3 Spoofing and Sniffing

Sniffing and spoofing are security threats that target the lower layers of the networking infrastructure supporting applications that use the Internet. Sniffing is a passive security attack in which a machine separate from the intended destination reads data on a network.

Spoofing is an active security attack in which one machine on the network masquerades as a different machine. As an active attack, it disrupts the normal flow of data and may involve injecting data into the communications link between other machines. This masquerade aims to fool other machines on the network into accepting the impostor as an original, either to lure the other machines into sending it data or to allow it to alter data.

7.3.4 Denial of Service Attacks

In computing, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet (source: Wikipedia).

7.3.5 Identity Theft

Identity theft is a form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity, usually as a method to gain access to resources or obtain credit and other benefits in that person's name. The victim of identity theft (here meaning the person whose identity has been assumed by the identity thief) can suffer adverse consequences if they are held responsible for the thief's actions as the thief can commit crime imposing as another victim.

7.3.6 Phishing

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. For example, an e-mail can be sent to the victim luring the victim to enter a site and when entered, information such as usernames, passwords and credit card information may be collected by the criminal posing as the victim's bank site.

7.3.7 Internal Employees

Employees who are dissatisfied with the organization may also steal confidential information as well as harm the organization by destroying information, stealing hardware etc. These employees are known as 'insiders'. In most cases, it is difficult to identify the insiders. Inappropriate insider behavior can be a bigger threat, both more common and often causing greater financial losses than outsider attacks.

7.4 **Measures to Address Security Concerns**

In order to properly manage information security, set of security controls such as authentication, authorization, integrity, privacy and non-repudiation should be established with the enterprise. The following section describes some of these security controls in detail.

7.4.1 Technologies and Tools Used for Security and control

This section looks at security tools and techniques for protecting information assets. Various computer security tools and techniques are available that address how to:

- Verify that users are who they say they are (authentication).
- Control access to data and functions (authorization).
- Protect the privacy and integrity of information assets (data privacy and integrity).
- Ensure non-repudiation, so parties can't deny their actions (non-repudiation).

Authentication
Authentication requires users to prove who they say they are. The most basic approach is to require users to provide information that, presumably, only they know, such as a ***user name and password***, their ***mother's maiden name***, or a ***Personal Identification Number (PIN)***. A second approach is to use something they possess to present proof, such as ATM card, smart card or authentication software. Still another approach to authentication utilizes ***biometrics*** such as, fingerprints, voice prints, retinal scans, etc. Biometrics involves the measurement of one of a person's traits which can be behavioural or physical. Biometrics can be used to limit physical access to computer equipment too. For example, access to a data center can be restricted by scanning individual traits and allowing only authorized persons to enter.

The simplest password authentication mechanism is the transmission of a password in the clear from the user to the server. However, simple password based authentication mechanism is vulnerable to various attacks.

Authorization
Used for access control purposes. Identification involves issuing entry privileges only to those individuals who require access to specific information or applications. Access Control is the most frequent mechanism of data protection, used extensively by computer security products. There are various systems for access control in both Local Area Networks (LAN) and Internet environments, and there is a growing demand for single, or reduced sign-on requirements to minimize the number of times that authorized users need to authenticate themselves.

Data privacy and integrity
This control involves preventing users from eavesdropping such as password-sniffing, viewing, tampering with or otherwise accessing unauthorized information. In general, eavesdropping attacks on a network can result in the theft of account information, such as credit card numbers, customer account numbers, or account balances and billing information. Password-sniffing attacks can be used to gain access to systems on which proprietary information is stored. Data modification attacks can be used to modify the contents of certain transactions (e.g. changing the payee on an electronic check or changing the amount being transferred to a bank account).

The most common approach to this problem involves ***encryption***, which makes information unintelligible to unauthorized users and provides an indication of any tampering. A common example of data privacy involves encrypting customers' credit card information when it is sent from their PC to a Web server. In other words data encryption allows a user to protect information so that others cannot read it. There are two set of algorithms called symmetric key algorithms and asymmetric key algorithms available in the area of cryptography to provide encryption. As mentioned these algorithms are out of the scope of this manual.

Non-repudiation
Preventing parties in a transaction from later denying things they said or did is an increasingly common requirement for computer security. Cryptographic techniques can provide proof that:

1. a message or order wasn't sent by an impostor, and
2. the intended addressee actually received the information.

Cryptography is the most powerful mathematical techniques related to above aspects of information protection. Cryptography is about the prevention and detection of cheating and other malicious activities. Basic cryptographic tools (primitives) used to provide information security is out of scope of this manual.

Other Security Measures

In addition to cryptography, tools such as ***virus scanners, firewalls and Intrusion Detection Systems (IDS)*** protect information assets. Anti-virus software can detect virus, prevent access to infected files and often eliminate the infection. These virus scanners, detect, and often disinfect, the virus only known to the scanner. Therefore, the virus scanners have to update regularly to recognize new viruses. Even if a latest virus scanner has been installed, it is a good idea to keep backups of all data and software, including the operating system. In principle, virus protection software should be configured to:

- scan computer memory, executable files (including macros contained in desktop software data files), protected files (eg compressed or password protected files) and removable storage media
- scan incoming and outgoing traffic (including e-mail and downloads from the Internet)
- be active at all times
- provide an alert when a suspected virus is identified
- disinfect, delete or quarantine viruses when identified
- ensure that virus protection features cannot be disabled or core functionality minimized.

Firewalls serve a valuable purpose in securing Internet-connected networks. However, they do not provide end-to-end transaction security and cannot be considered adequate security solutions for commercial Internet transactions.

IDS are some kind of network monitoring software tools that can be used to sound alarms, alerting security staff when suspicious activity occurs. Intrusion detection software should include:

- detection of known attack characteristics (eg denial of service or buffer overflows)
- a process for performing regular updates to intrusion detection software, to incorporate new or updated attack characteristics
- provision of alerts when suspicious activity is detected, supported by documented procedures for responding to suspected intrusions protection of intrusion detection mechanisms against attack, such as isolation on a separate network.

It's a good idea to maintain an audit trail of user activity, both at firewalls and on Web and application servers. Audit trail log files should be examined on a regular basis by security staff to determine if unauthorized activity has taken place; these log files should typically be archived for a year or so.

Above discussed techniques and tools cannot alone provide information security. ***Limiting physical access*** to servers, routers and other systems is obviously a good idea. In a similar vein, by physically reorganizing or consolidating information assets, we can simplify the management of those assets while increasing their security. For example, moving the customer and order databases to their own server makes it easier to control access and manage those specific assets. These servers and the other computer infrastructures should also be physically protected as follows:

Workstations: Users should consider methods such as cables, locks, bolts for attaching equipment to desktops to prevent computer workstations and associated peripherals are stolen.
Laptops: Since laptops are easily stolen, users should require a locking cable or an alarm to prevent theft. Users should never leave portable computers unattended.
Servers: In general, servers should be isolated and made accessible only to system administrators and appropriate IT staff. Depending on the nature of the information stored on the servers, it may be appropriate to locate the server in a locked room or other access-controlled environment.
Network infrastructure: In a similar fashion, routers, firewalls and other computer network infrastructure systems should be isolated and available only to appropriate IT staff.

7.4.2 Security Policy

Keeping the business risks associated with information systems under control within an enterprise requires clear direction and commitment from the top management, the allocation of adequate resources, effective arrangements for promoting good information security practices throughout the enterprise and the establishment of a secure environment.

In principle, top management of an organization should demonstrate their commitment to information security by:

- setting direction for information security (eg by an information security policy)
- assigning overall responsibility for information security to a top-level director or equivalent
- chairing key information security working groups
- monitoring the security condition of the enterprise
- allocating sufficient resources to information security.

A comprehensive, documented information security policy should be produced and communicated to all individuals with access to the enterprise's information and systems. Staff should be educated on information security and an agreement should be established that specify information security responsibilities are incorporated into staff agreements.

There should be an individual (or a group of individuals) responsible for maintaining the security policy. The information security policy should define information security, associated responsibilities and the information security principles to be followed by all staff. It should also state that disciplinary actions may be taken against individuals who violate its provisions. The information security policy should be reviewed regularly according to a defined review process and revised to take account of changing circumstances.

In principle, a high level information security policy should prohibit:

- using the enterprise's information and systems without authorization or for purposes that are not work related
- making sexual, racist or other statements, which may be offensive
- making obscene, discriminatory or harassing statements, which may be illegal
- downloading illegal material (eg with obscene or discriminatory content)
- the movement of information or equipment off-site without authorization
- unauthorized use of information, facilities or equipment
- unauthorized copying of information/software
- compromising passwords (eg by writing them down or disclosing them to others)
- using personally identifiable information for business purposes unless explicitly authorized
- discussing business information in public places
- tampering with evidence in the case of an incident.

In addition, such information security policy should state that users should:

- lock away sensitive media or documentation when not in use
- log-off systems in use when leaving a terminal/workstation unattended

7.4.3 Security Audit

The information security status of critical IT environments should be subject to thorough, independent and regular security audits/reviews. Independent security audits/reviews should be performed periodically for critical environments, including business applications, computer installations, networks, systems development activities and key enterprise-wide security activities. In

principle, security audits/reviews should be:

- defined in scope, and documented
- performed by qualified individuals who have sufficient technical skills and knowledge of information security
- conducted sufficiently frequently and thoroughly (in terms of scope, extent) to provide assurance that security controls function as required
- focused on ensuring that controls are effective enough to reduce risks to acceptable levels
- checked by competent staff
- complemented by reviews conducted by independent third parties.

7.5 Ethical Issues

It is well known that IT has caused many negative effects on the society and people in each of the cases as stated under security threats. Obviously, computerization of a manual process leaves loss of jobs while the working conditions and efficiency are improved with reduced current cost.

7.5.1 Overview of Ethical Dimensions

There are important challenges that come up from the use of information systems and technologies in business. These challenges are in the areas of

- employment
- workplace privacy
- conditions in the workplace
- individuality of people
- health

Employment Challenges [Ref 2: pp 393-394]
Information technology has led to creating new jobs and increased productivity. However, it has also caused significant reduction in some types of jobs and opportunities.

For example, when we use automated machines to carry out activities like painting, fixing of components in a car assembly line, number of people required to carry out these activities is reduced. This leads to job losses. Further, use of information systems and technologies may require different type of skills and knowledge. Therefore, workers should be trained in these areas. The workers may be unemployed unless they can be retrained for new positions or new responsibilities.

Privacy Issues
Privacy issues has been discussed under section 7.2.
Management should be sensitive to the privacy of customers as well as employees. Disclosing private information of customers for monitory gain etc., violates the privacy of employees. Similarly employee privacy may also be violated by implementing concepts such as employee monitoring via the use of computers.

Computer monitoring **[Ref 2: pp 394-395]** is the use of computers to monitor the productivity and behaviour of employees while they work. This is one of the most explosive ethical issues concerning workplace privacy and the quality of working conditions in business. While it is argued that computer monitoring enables to monitor employee productivity.

It is considered unethical because it continually monitors individuals violating the workers privacy and personal freedom. For example, an employee working in a help desk may be monitored on the exact number of seconds she took to respond to the caller and the number of minutes taken to

provide a solution. The conversation may also be recorded and monitored.

Computer monitoring is considered as an invasion of privacy as in many cases, the employees are not aware that they are being monitored. Furthermore, computer monitoring is blamed for creating employee stress due to continually working under electronic surveillance. In these environments in some cases, workers are forced to work at a hectic pace under poor working conditions.

In some countries such as United States, political pressure is leading to regulating computer monitoring in workplace. Several laws have been proposed for this purpose.

Impact on Working Conditions [Ref 2: pp 395]
Due to the introduction of information systems and technologies to the work environment, employee job roles have improved in some cases. For example, in the automobile industry many of the monotonous obnoxious tasks such as repetitive welding and spray painting jobs are being carried out using robots. This has led to people concentrating on more challenging and interesting job roles.

On the other hand, information technology has led to creating jobs which are quite repetitive and routine. For example, data entry. In some cases due to the introduction of information technology in assembly-line operations employees are forced to work like machines. Further, due to automation people are employed to carry out activities like pressing buttons infrequently. This type of jobs does not improve creativity of employees nor are challenging.

Effects on Individuality [Ref 2: pp 395]
Computer based information systems are often criticised for the negative effect on the individuality of people. One of the reasons is due to the elimination of human relationships present in non computer systems. Another aspect is requiring individuals who possess skills and capabilities to function computer systems which are often inflexible.

Health Issues [Ref 1: pp 706-708; Ref 2: pp 395-396]
A variety of health issues are raised by the use of information technology in the work place. Common health problems created through heavy use of computers include eye strain, back pain, damaged arm and neck muscles. Computer monitoring is also considered as a major cause of job stress.

People involved with repetitive key stroke jobs can suffer variety of health problems known as Cumulative Trauma Disorders (CTDs). In such situations, workers fingers, wrists, arms. Necks and back may cause severe pain. Carpel tunnel syndrome which is common among typists is a painful, crippling ailment of the hand and wrist that typically requires surgery to cure. Eye strain can also be caused due to viewing of video displays for a long period of time.

In order to address the health issues associated with the use of information systems several remedies are proposed. Ergonomics is the study of designing of healthy, safe, comfortable and pleasant work environments.

7.5.2 Business and Technology Ethics

As we discussed above information technology has beneficial as well as detrimental effects on society as well as on people. Therefore, the management of an organisation should take steps to reduce the negative effects and improve the working conditions of the employees.

Many organisations have developed policies to address the ethical issues discussed in sub section

7.5.1 arisen due to use of information systems. In order to address these issues, a code of conduct is developed by the Association of Information Technology Professionals (AITP), an organisation of professionals in the computing field. By following these guidelines voluntarily IS professionals can live up to their ethical responsibilities.

Based on the AITP code of conduct, you can be a responsible professional by (1) acting with integrity (2) increasing professional competence (3) setting high standards of personal performance (4) accepting responsibility for your work (5) work towards improving the health, privacy and general welfare of the public.