Course Overview

INTRODUCTION

Welcome to CCS200, Computer Security. This is a one-semester course with three credit hours that should be completed in a period of 15 weeks. This subject is offered to under graduate level course for Asia e-University students in Bachelor Degree in Information Technology (Security). The contents, activities, self-check and discussion questions in this module will help students to master the topics over a period of one semester.

PURPOSE OF THIS COURSE GUIDE

Students are expected to have basic knowledge on the study skills required for open distance learning at Asia e-University. Students are required to read this Course Guide thoroughly before looking at the module.

This Couse Guide tells students briefly what the course is all about and how students can work with their way through the material. It suggests the amount of time students will need to spend to complete the module, activities and exercises need to carry out and how good to allocate their time in mastering the contents of this module.

COURSE AIMS

The aim of CCS200 is to provide understanding and exposure to students regarding Computer Security Concepts, Security Framework, Authentication, Prevention and Technical Defense in computer and networking working environment.

COURSE OBJECTIVES

At the end of this course, students should be able to:

- Understand the provision of computer security in safeguarding the information systems;
- Identify the threats and vulnerabilities to the information systems;
- Appreciate issues that arise in devising practicial solutions to management of computer security for information system requirements;
- Protecting information infrastructure by applying prevention and technical defences; and
- Describe the risk management, risk assessment and risk analysis.

STUDENT STUDY PLAN

The Asia e-University study approach requires students to fullfill 42 hours of independent study and the total of 120 learning hours. The estimation time allocation that help students to divide their study time shown in Table 1.

Table 1: Estimation Time Allocation for CCS200 Computer Security

Activities	Hours
Independent Study	42
Tutorial/Face-to-face Interaction	12
Online Interaction	30
Assignments	18
Examination Preparation	18
TOTAL	120

MODULE STRUCTURES

There are nine major chapters in this module. A brief summary of each chapter given as below:

CHAPTER 1 Fundamentals of Computer Security

This chapter discusses the brief history of computer security and its important. In order to implement the computer security, it is very important for organisations to properly develop and established their policies, procedures, standards and guidelines to maintain the security of the systems and network.

CHAPTER 2 Authentication and Basic Cryptography

Chapter 2 looks at the important of an authentication process. An authentication is related to the scenario where some party (claimant) has presented a principal's identity and claims to be that principal. Authentication enables some other party (verifier) to gain confidence that the claim is legitimate.

CHAPTER 3 Threats and Vulnerabilities

Computer vulnerability is a weakness in an operating system, application code, or configuration that makes it possible for threats to exploit the system (or underlying network) thereby creating negative impact or damage. Threats are entities that act upon vulnerabilities for the purpose of trying to exploit it. A threat may be an unauthorised user such as a hacker, or even a system administrator trying to obtain access above and beyond their authorised level of privilege.

CHAPTER 4 Prevention and Technical Defenses

This chapter discusses about the important of protecting infrastructure from disaster especially for industry, government and society. Yet with more activities dependent on computer networks - from banking and aviation to emergency services - the reliability and security of information and communication systems against disasters, both natural and man-made, are in doubt.

CHAPTER 5 Detection

This chapter discusses the important of rapid detection and appropriate notification of any security strategy. Intrusion detection is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. Without proper detection, you may never be aware that a security incident has occurred and thereby continue to use corrupt information to make business decision.

CHAPTER 6 Social Engineering

Chapter 6 discusses about the responsibilities of a security professional in today's ever-changing world, it is important to be familiar with Social Engineering techniques and the counter-measures available to reduce the likelihood of success. By having this knowledge, one can ensure appropriate the preventative, detective and corrective measures are implemented to protect the staff and assets of an organisation.

CHAPTER 7 Human Factors

This chapter discusses about the implementation of right IT security concept where it can assist users in building a solid basis for a level of IT security that users 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).

CHAPTER 8 Risk Management

Risk management can best be described as a decision making process. Industry best practices clearly indicate that an important aspect of effectively managing risk is to consider it an ongoing process. Effective risk management avoids costly over-sights and unexpected problems.

CHAPTER 9 Implementation (Delivery) Options

This final chapter discusses about the Security Assurance where it is critical for determining trust worthiness of systems. Different levels of assurance arise, from informal evidence to rigorous mathematical evidence. Assurance needed at all stages of system life cycle and building security in is more effective than adding it later.

READING MATERIALS

Some of important reading materials that could help students to understand this course in detail given as below:

1. Seymour Bosworth and Michel E. Kabay (2002), Computer Security Handbook 4th Edition, John Wiley & Sons.
2. Charles P. Pfleeger, Shari Lawrence Pfleeger (2003), Security in Computing, Prentice Hall PTR.
3. Matt Bishop (2003), Computer Security: Art and Science, Addison-Wesley.
4. Ross J. Anderson (2008), Security Engineering: A Guide to Building Dependable Distributed Systems, John Wiley and Sons.
5. William Stallings (2003), Network Security Essentials: Applications and Standards, Pearson Education.

CHAPTER 1

Fundamentals of Computer Security

LEARNING OUTCOMES

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

1. Define the meaning of security in computer systems;
2. Determine security problems associated with computer systems;
3. Explain the general computer security framework concepts; and
4. Identify the trends and issues in computer security.

INTRODUCTION

Let us look at the article given below.

Scareware Arrives on Twitter in Latest Attack

As new Web 2.0 threats proliferate, business IT departments struggle with basic tasks such as patch management. *June 3, 2009; By Alex Goldman*

Be careful of links in Twitter. The latest malware attack on the social network links to a video hosted on a site that installs scareware as victims watch the video. The attack may be linked to a previous phishing attack on Twitter that exploited the deceptive domain name "tvvitter.com" to obtain victims' Twitter credentials. At the time, Sophos security expert Graham Cluley noted on his blog that careful users of a browser plug-in called LongUrl would have been able to see that the link was deceptive. But apparently many were fooled.

"They used the stolen credentials to post a message about finding a good video," Yuval Ben-Itzhak, CTO of Web security company Finjan, told Internet-News.com. "If you clicked on the link ... the criminals installed rogue anti-spy-ware called System Security."

Criminals are making money from scareware. Finjan's Malicious Code Research Center recently published a report, "Cybercrime Intelligence Report: Cybercrime pays generously," that estimated that hackers can earn $10,800 a day from rogue anti-virus software, and that's before they sell their victims' credit card numbers on online criminal markets.

The news comes as IT departments are unprepared for the security threats posed by Web 2.0, according to reports. A Kaspersky researcher warned about Twitter links at Interop last month.

Ben-Itzhak agreed. "The problem is not just Twitter but any user-generated content site. If you let users upload content and include links, you can end up with malicious content installed on your machine."

He had some advice for IT managers. "Organizations and corporations should be aware that Web 2.0 and user-generated content sites can add value and increase productivity, but at the end of the day, if they're not protecting users from these attacks, they're not protecting their own network."

He said companies cannot rely on traditional anti-virus systems that use signature detection to block malware. "They need real time content inspec-tion technologies," he said. "It's unlikely that anti-virus vendors will have a signature for something that someone just created and put on Twitter."

It's a real challenge, and many IT organizations are not up to the task. A recent report from Sophos said that nine out of ten at-work PCs fail basic security tests, such as being up to date on operating system patches.

Source: http://www.internetnews.com/webcontent/article.php/3823246

Based from the article given, identify the issues faced by the IT organisations and the causes of these problems.

Computer security is a branch of technology known as information security as applied to computer(s). Information security involves the security in an organisation regarding the application security, policies involves and IT infrastructure to create a secure and protected computing environment for an organisation.

Traditionally, information security has been considered to have three fundamental objectives, namely:

- Confidentiality (C);
- Integrity (I); and
- Availability (A).

In contemporary computer network environments, another fundamental objective that should be covered is legitimate use of resources which is ensuring that resources are not used by unauthorised persons or in unauthorised ways.

Computer security is the process of preventing and detecting unauthorised use of computer. Prevention measures help to stop unauthorised users or intruders from accessing any part of computer system. Detection helps to determine whether or not someone attempted to break into system.

1.1 HISTORY OF COMPUTER SECURITY

Identity theft is common today as there are various ways to attack computers and networks. By looking at some of the crimes that have been committed over the last few years, it can be clearly understood the threats and security issues has surrounded the computer systems and networks.

Fifty years ago, only a few people had access to a computer system or a network. Securing these systems was easier back then. Furthermore, many companies did not conduct business over the Internet.

Nowadays, companies are very much relying on the Internet to operate and conduct businesses. Companies used networks to transfer huge amounts of money in the form of bank transactions or credit card purchases. Whenever the money is transferred through networks, hackers try to take an opportunity of network environment to perform fraud or theft.

Electronic crimes can be defined in many forms. This chapter will concentrate on two basic categories, which are the crimes in which the computer was the target and incidents in which a computer was used to commit the act. The first real internet crime case was started in 1988 Internet Worm by Robert Morris. The chronology of the incidents are shown in Table 1.1, Table 1.2 and Table 1.3.

Table 1.1: Chronology of the Computer Security Incidents (1988 – 2003)

Year	Incident	Descriptions
November 1988	The Morris Worm	Robert Morris, a graduate of Cornell University, released The Internet Worm (or the Morris Worm). The worm infected 10 percent of the machines (approximately 6,000) connected to the Internet at that time. The virus caused an estimated $100 million in damage, though this number has been the subject of wide debate.
June – October 1994	Citibank and Vladimir Levin	From June 1994 through October, Vladimir Levin, of St. Petersburg, made a number of bank transfers. When he and his accomplices were caught, they had transferred an estimated $10 million. Eventually all but about $400,000 was recovered. Levin reportedly accomplished the break-ins by dialing into Citibank's cash management system.
February 1995	Kevin Mitnick	Kevin Mitnick's computer activities occurred over a number of years from the 1980's through 1990's. Mitnick admitted to having gained unauthorised access to a number of computer systems belonging to companies such as Motorola, Novell, Fujitsu and Sun Microsystems.

Table 1.2: Chronology of the Computer Security Incidents (1988 – 2003)

Year	Incident	Descriptions
July 1996	Omega Engineering – Timothy Lloyd	• On July 30, 1996, a software "time bomb" at Omega Engineering deleted all design and production programs of the company. This severely damaged the small company forcing the layoff of 80 employees. • The program was traced back to Timothy Lloyd who had left it in retaliation for his dismissal.
March 1999	Melissa Virus	• Melissa is the best known of the early macro type of virus that attaches itself to documents, which contain programs with a limited macro programming capability. • The virus was written and released by David Smith. • This virus infected about a million computers and caused an estimated $80 million in damages. • This virus clogged networks with the traffic and caused problems for e-mail servers worldwide. • It attached itself to Microsoft Word 97 and Word 2000 documents. • Whenever a file was opened, a macro caused it to infect the current host and also sent itself to the first fifty addresses in the individual's address book. • To avoid infection by Melissa, users should not open the attached file.
May 2000	Love Letter Worm	• The worm spread via e-mail with the subject line "ILOVEYOU." • The number of infected machines worldwide may have been as high as 45 million. • Similar to the Melissa virus, the Love Letter Worm spread via attachment to e-mails. In this case, instead of utilising macros, the attachments were VBScript programs.

2001	Code-Red Worm	• On July 19, 2001, over 350,000 computers connected to the Internet were infected by the Code-Red worm. The incident took only 14 hours to occur. • Damages caused by the worm (including variations of the worm released on later dates) exceeded $2.5 billion. • The vulnerability exploited by the Code-Red worm had been known for a month.

Table 1.3: Chronology of the Computer Security Incidents (1988 – 2003)

Year	Incident	Descriptions
August 2001 - May 2002	Adil Yahya Zakaria Shakour	Shakour accessed several computers without authorisation, including: • Eglin Air Force Base (where he defaced the web site). • Accenture (a Chicago-based management consulting and technology services company). • Sandia National Laboratories (a Department of Energy facility). • Cheaptaxforms.com • At Cheaptaxforms.com, Shakour obtained credit card and personal information, which he used to purchase items worth over $7,000 for his own use.
2003	Slammer Worm	• The Slammer virus was released on Saturday, January 25, 2003. • It exploited buffer-overflow vulnerability in computers running Microsoft's SQL Server or Microsoft SQL Server Desktop Engine. • This vulnerability was not new. • It had been discovered in July 2002. • Microsoft had released a patch for the vulnerability even before it was announced.

- By the next day, the worm had infected at least 120,000 hosts and caused network outages and disruption of airline flights, elections, and ATMs.

Use the internet to search for more history on computer security. Share your findings with the other students.

1.2 WHAT IS COMPUTER SECURITY?

Security measures fall into several categories. Computer security is the protection of information within a computer system and it embraces such subcategories as operating system security and database security. Computer security measures need to interwork with security measures in other categories, such as communications security, physical security and personnel security.

Computer security has three objectives. It can be independent or overlap and mutually exclusive. To understand further, these terms are displayed and explained in Table 1.4.

Table 1.4: Objectives of Computer System Security

Objective	Definition
Confidentiality (C)	Ensuring that information is not disclosed or revealed to unauthorised persons and computer-related assets are accessed only by authorised parties.
Integrity (I)	From June 1994 through October, Vladimir Levin, of St. Petersburg, made a number of bank transfers. When he and his accomplices were caught, they had transferred an estimated $10 million. Eventually all but about $400,000 was recovered. Levin reportedly accomplished the break-ins by dialing into Citibank's cash management system.
Availability (A)	Ensuring that legitimate users are not unduly denied access to information and resources and assets are accessible to authorised parties at appropriate times.

The relationship between these three objectives can be seen in Figure 1.1.

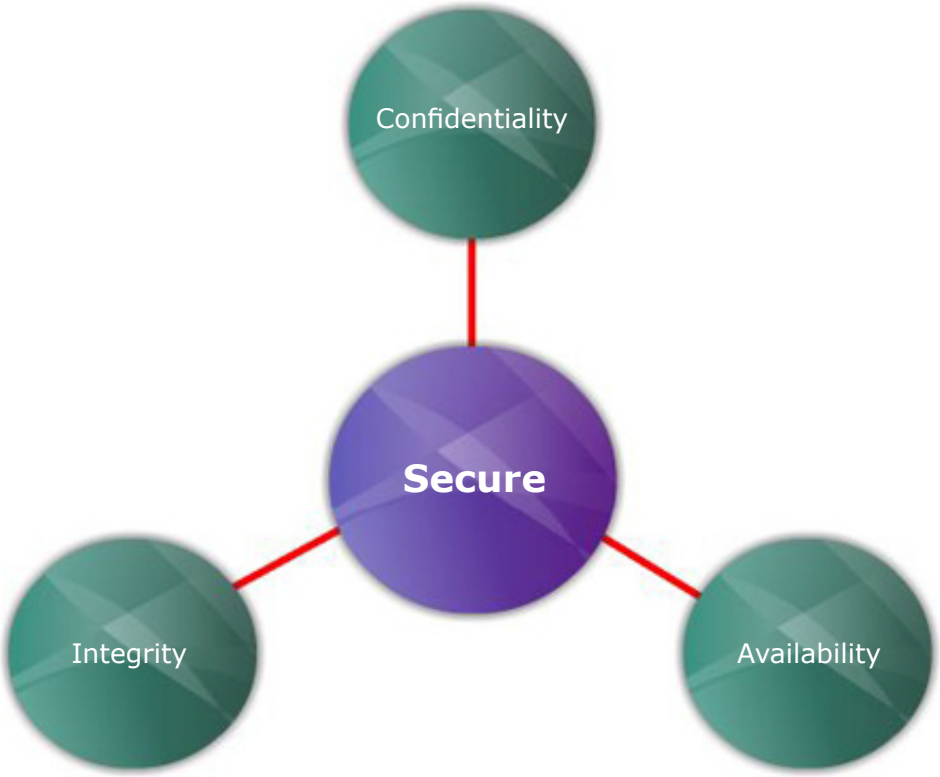

Figure 1.1: Relationship between the three objectives

From the Figure 1.1 above, we will break down each of the objectives into details as shown in Table 1.5.

Table 1.5: Explanation on the Relationship between the Three Objectives in Computer Security

Objective	Descriptions
Confidentiality	• Generally, the main objective of computer security is to stop unauthorised users reading sensitive information. Confidentiality (privacy and secrecy) captures this aspect of computer security. • The terms 'privacy' and 'secrecy' are sometimes used to distinguish between the protection of personal data (privacy) and the protection of data belonging to an organisation (secrecy). • Sometimes security and confidentiality are used as synonyms.
Integrity	• Normally, integrity is about making sure that everything is as it is supposed to be.

	• Integrity deals with the prevention of unauthorised writing. • In this interpretation, integrity is the dual of confidentiality and we can expect to use similar techniques to achieve both goals. • If one would equate integrity with the prevention of all unauthorised actions then confidentiality becomes part of integrity. • Integrity is often prerequisite for other security properties. • For example, an attacker could try to avoid confidentiality controls by modifying the operating system or an access control table referenced by the operating system. • Hence, we have to protect the integrity of the operating system or the access control table to achieve confidentiality. • However, there are even more general definitions of integrity, which treat security and availability as parts of integrity.
Availability	• Availability is very much concern ahead of the traditional boundaries of computer security. • In the context of computer security, availability has to ensure that a malicious attacker cannot prevent legitimate users from having reasonable access to their systems or denial of service. • There have been incidents of flooding attacks on the internet where the attacker effectively disables a server by overwhelming it with connection requests. • In many cases, availability can be the most important aspect of computer security, but there is a distinctive lack of security mechanism for handling this problem. • In conclusion, too restrictive security mechanism can lead to denial of service.

SELF-CHECK

1. What is the definition of data confidentiality, data integrity and data availability?
2. List two threats that can be used to damage the data confidentiality, data integrity and data availability.
3. Data integrity can also be threatened by environmental hazards such as dust, surges and excessive heat. True or False?

1.3 SIGNIFICANCE OF COMPUTER SECURITY IN THE ORGANISATIONS

In any security-aware organisations, computer security is closely related to operations and organisational security. The organisations will design prevention technologies to keep individuals from gaining access to systems or data that they are not authorised to use. However, in the operational environment, relying on prevention technologies only was not acceptable as it will led to rise of technologies that can detect and respond to unauthorised events but at the same time the prevention is failure.

In order to implement the computer security, it is very important for organisations to properly develop and established their policies, procedures, standards and guidelines which consist of what the users and administrators can do to maintain the security of the systems and network. These documents can provide the guidance needed to implement the security in the organisations.

Therefore, the specific technology and security mechanisms required can be well-planned before implementing systems and network. This document is elaborated as displayed in Figure 1.2.

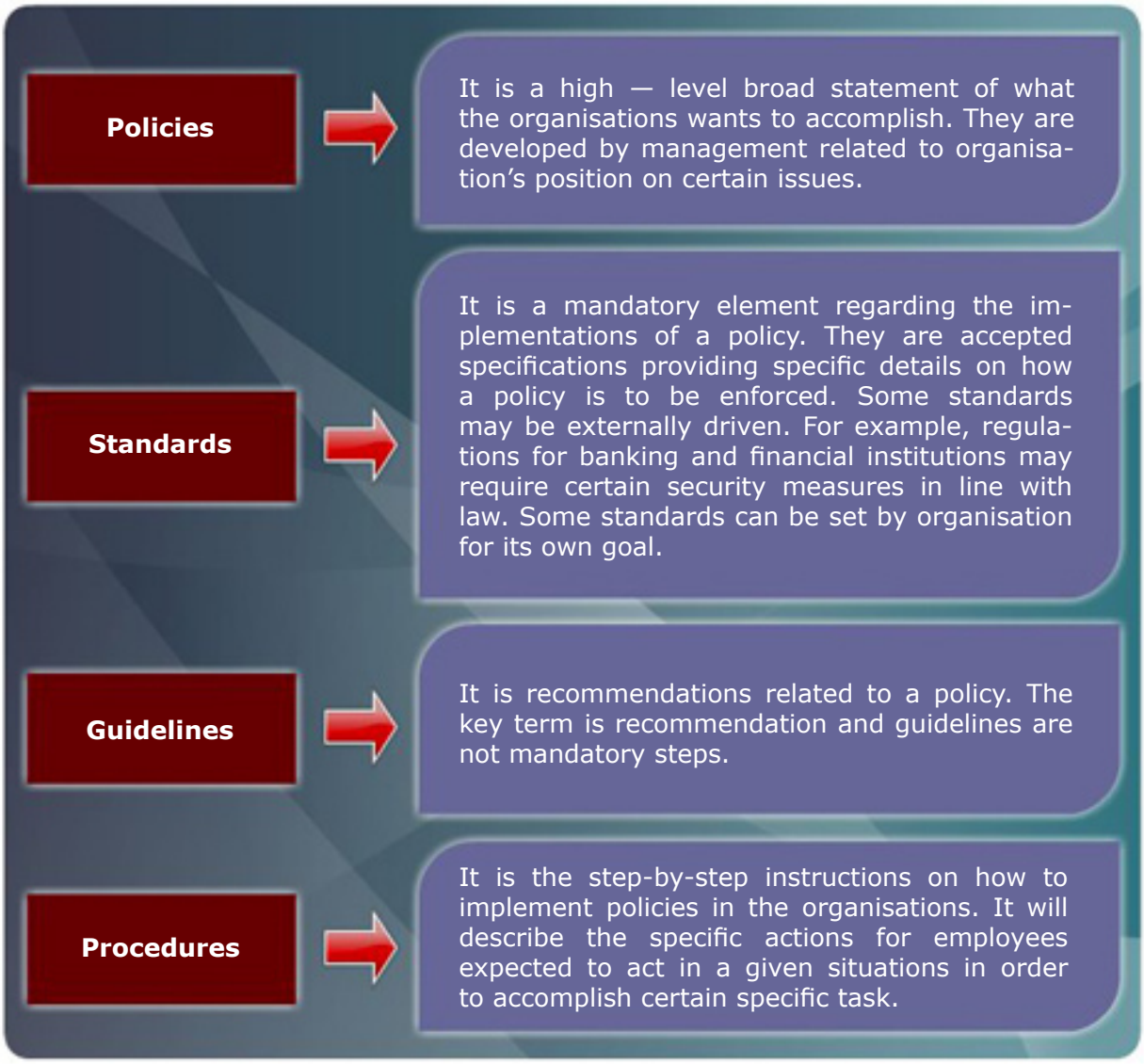

Figure 1.2: Significance of computer security in organisations

Due to the constantly technologies changes, the documents should be periodically review and evaluated. Document changes are accepted if necessary. This process is known as the policy life cycle and its operational process can consists of four steps which is Plan (Adjust), Implement, Monitor and Evaluate. The diagram of the process is shown in Figure 1.3, followed by explanation on each of the process.

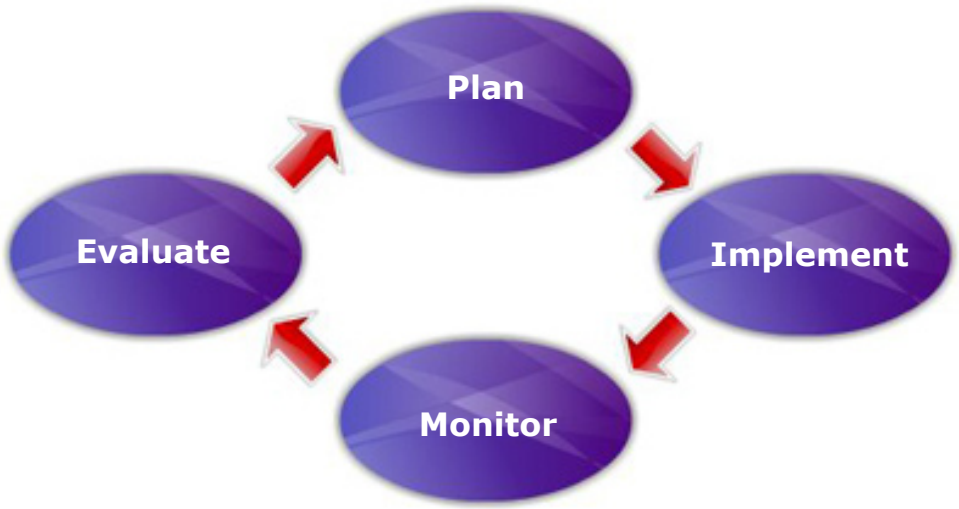

Figure 1.3: Policy life cycle

1. **Plan** – This first step requires you to develop the policies, procedures and guidelines that will be implemented and design the security component that will protect your network.

2. **Implement** – Once the development has been done, the plan can be implemented. There will be an instruction period where those who will affect by the change of this new document will learn about its content.

3. **Monitor** – This step is needed to ensure that both of the hardware and software as well as the policies, procedures and guidelines are effective enough in securing your systems.

4. **Evaluate** – The document shall be evaluated to verify the effectiveness of the security measures. It should include vulnerability assessment, penetration test of your system to ensure the security is adequate. After evaluating your security posture, you can go through step 1 again and adjust the security mechanism as per requirement.

1.4 COMPUTER SECURITY FRAMEWORK

Most of the damage to computer security is not from outside malicious attacks, but rather from simple mistakes, unintended or unauthorised actions of legitimate users and administrators who are either untrained in security and/or who misunderstood the instructions from the management.

The two major issues mentioned replay themselves daily in the IT world. Part of the

reason this is happening is a lack of common, proven practices and guidelines developed for IT professionals. Unlike the legal, financial, and medical fields, the IT field is still somewhat in its infancy. It has yet to develop the kind of respect from the business community that legal, financial, and medical professionals enjoy, despite the fact that IT professionals are increasingly tasked to handle and protect the core values of the organisation which are data and information that legal, financial, medical professionals, and management depended on.

There is no question how important the IT department is for any organisation. So what are the issues when it comes to poor security in most computer security operations? The following Table 1.6 shows a few main issues regarding the computer security framework.

Table 1.6: Computer Security Framework Issues

Example	Main issues
Management vs System Users vs IT Professionals	• When it comes to computer security, management, system users, and IT professionals are often at odd as to what is the best course of action in response to a given security concern. • Management usually understands the high-level issues; users generally want convenience; and IT of course wants to please the first two while still doing their job. • However, they do not have a common framework to follow, and most do not have a common policy to follow. • To make matters worse, everyone believes their way is the best, regardless of the real over-riding issues.
Standards	• There is a total lack of standards when it comes to computer security. • Others profession such as Certified Public Accountant or Attorney has their own ideas regarding what the standards are. • These groups may even change the standards from time to time in response to a given situation, even though next time around it could be different. • Things are done to solve an "urgent" issue with an intention to revisit the actions taken later, when the urgency is over.

Complexity of the Information Technology	• Supporting the current IT infrastructure is exponentially more difficult than it was ten years ago. • While supporting the hardware aspect of IT has gotten dramatically easier, supporting the rest of the IT infrastructure is much more difficult today than it was in the past. • Most management and system users do not appreciate how difficult is to keep the IT operation running smoothly. • Management as well as system users only see the front end of the IT system which is GUI windows but at the back end, IT is facing increasingly complex configurations and environments to make everything work. • Nearly all operating systems and most applications today use different security standards.
Consistency	• Until just a few years ago, there was not a concerted effort in the IT industry and among IT professionals to focus on security. • Even most training focuses on a micro-level that is specific to the given products and at times, a given task. • Very few IT professionals have a comprehensive knowledge of all the levels of IT security necessary for them to be able to perform their job consistently, each and every time. • Without a high-level IT security framework and/or IT security policy, the security tasks will be performed by an individual IT professional based on his or her unique experience. • The results are often mixed and may or may not even be desirable. • At best, even if the security tasks are performed by the same individual, the results can be inconsistent.

Policy	• Most of the organisations today either still do not have a well defined security policy or none is ever developed at all. • Where there is a comprehensive security policy, it is not well communicated and /or enforced because it lacks high-level framework to guide it. • Very often the policies address security issues at a micro-level that are hard for management, system users, and IT professionals to understand or enforce consistently. • For the organisation that has a well defined security policy, very often there is not a well trained team which consists of all stakeholders that can enforce and fine-tune it, hence over time the system breaks down.
Framework	• For an IT security system to work, more needs to be done. • A well defined framework needs to be developed involving all stakeholders, and it needs to be self-tuning over time to be useful. • Almost all of the organisations today have a good framework and most understand the need for a well defined security policy to enforce and fine-tune the IT security system, but unfortunately, most stop there after they have developed one. • Refer to Figure 1.4 which shows a general high-level view of the security framework and brief overview of each step.
Training	• One major difference between traditional, well respected professionals such as Medical Doctors, Attorneys and the IT practitioner is the IT practitioners' lack of a structured approach to learning their trade. • There is not a well defined curriculum developed for people who intend to go into IT fields. • Most IT trainings are mainly focused on product-specific and commercial aspects of the subject matter, combining marketing and product promotion as part of the training. • Traditional curricula that produce the skills demanded of most computer programmers and en-

gineers are not suitable for keeping up with today's IT demands.

- In order for any IT security system to work, a well defined, organisation-wide security framework needs to be implemented that involves all stake-holders, and the framework needs to be part of the organisation's core operations at all levels of the organisational structure.

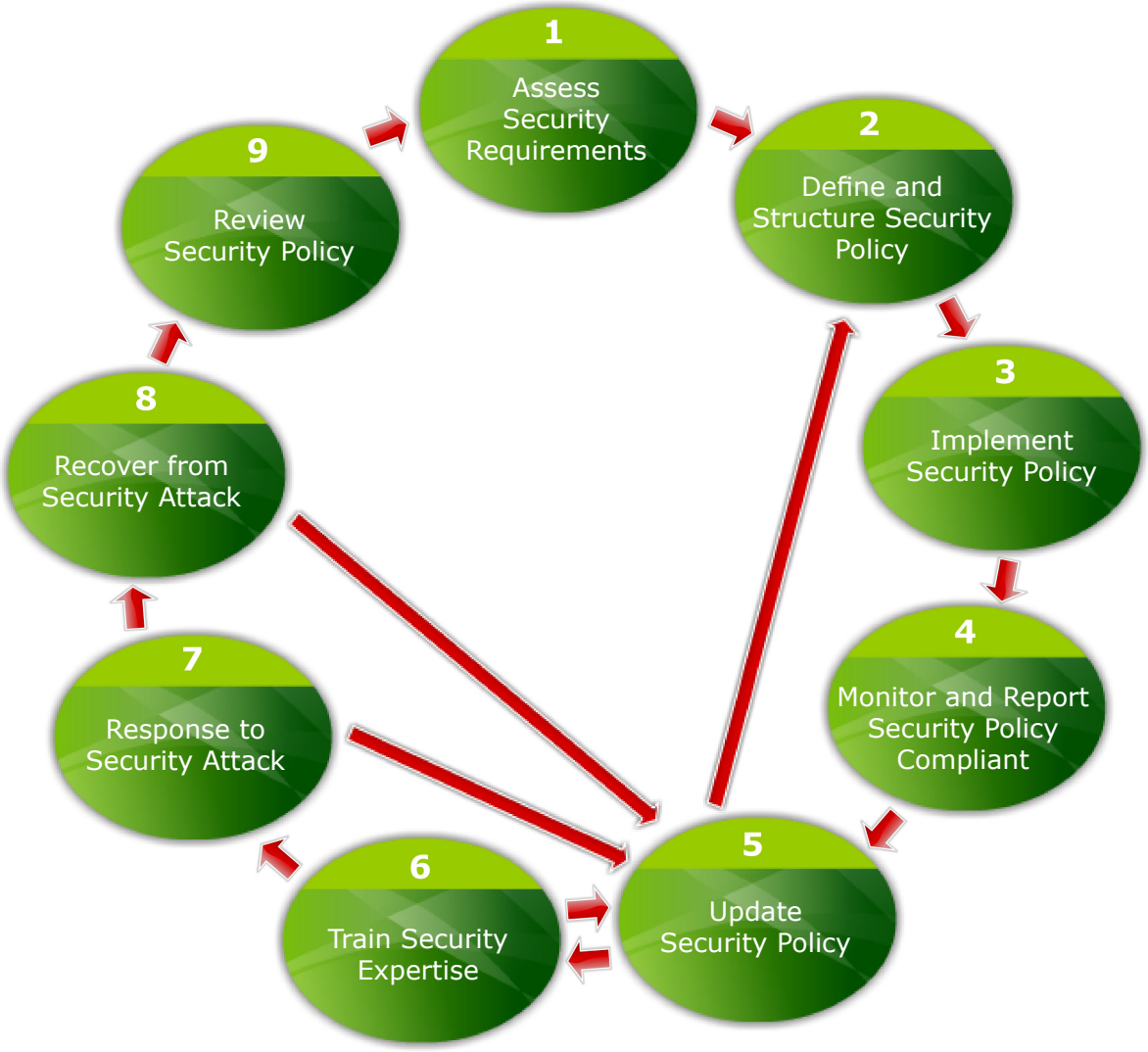

Figure 1.4: Computer security framework

From Figure 1.4, let us look into details each of the components in computer security framework.

1. **Assess Security Requirements** - Based on Business Processes, Business Needs, Business Environment, and Vulnerability Assessment on Both Network & Operating System and Penetration Test on Both Network & Operating System.

2. **Define & Structure Security Policy** - Based on Business Processes, Business Needs, Business Environment, Vulnerability Assessment on Both Network & Operating System and Penetration Test on Both Network & Operating System.

3. **Implement Security Policy** - Based on Business Processes, Business Needs, Business Environment, Vulnerability Assessment on Both Network & Operating System and Penetration Test on Both Network & Operating System.

4. **Monitor and Report Security Policy Compliant** - Based on Real-Time Known & Well Defined Events, On-Demand Developing & New Events and Regular Reviews.

5. **Update Security Policy** - Based on Changing Business Processes, Changing Business Needs, Changing Business Environment and Changing Technologies.

6. **Train Security Expertise** - Based on Changing Business Processes, Changing Business Needs, Changing Business Environment and Changing Technologies.

7. **Response to Security Attack** - Based on Real Time Intrusion Detection, Real Time Intrusion Response, Systems Operating System Hardening, Forensics Investigation and Litigation Support.

8. **Recover from Security Attack** - Based on High-Availability Systems Design and Disaster Recovery Plan.

9. **Review Security Policy** - Based on Changing Business Processes, Changing Business Needs, Changing Business Environment and Changing Technologies.

Now, let us look at one article taken from the internet in Figure 1.5.

CASE STUDY: SECURITY FRAMEWORK

By Paul Kapustka, ChannelWeb
Tue. Oct. 18, 2005
Cisco Systems (NSDQ:CSCO) is scheduled to add several features to its networked security framework today, including support for the company's popular Catalyst network switches as well as its wireless routers, according to Cisco.

The two-year-old framework, dubbed Network Admission Control (NAC), is Cisco's overarching plan for combining technologies and strategy to develop networks that can deploy security tactics automatically, by blocking or restricting devices that aren't compliant with network security policies. Previously, Cisco's NAC offerings included router software and standalone network appliances which communicated with PC "agent" software to determine whether client devices had the correct configurations and clearance.

By adding NAC support to Catalyst switches, Cisco customers can extend the framework's granularity down to the LAN level, said Cisco's Joe Sirrianni, a senior solutions manager for NAC. With NAC capability integrated into the switch's operating system, Sirriani said, administrators can make decisions (such as to isolate network elements that may have been infected by a worm or a virus) at the port level.

"There's a flexibility there now to do whatever fits [the situation] best," Sirriani said. The NAC framework will be available for Cisco's Catalyst 6500, 4900, 4500, 3700, 3500 and 2900 series of switches, and is scheduled to ship by the end of November as an operating-system software upgrade. Customers with appropriate switch support contracts, Cisco said, will get the NAC upgrade free.

Cisco is also scheduled to announce immediate availability of NAC framework support for its wireless routers, including its Aironet access points, also as a software upgrade free to customers with existing support contracts. Cisco also announced a new version of its standalone NAC appliance that supports single sign-ons for NAC and VPN access, as well as a new partner program to extend NAC support to client devices (such as IP phones or PDAs) that might not have the memory or processing capability to house Cisco's Trust Agent client software.

The company also said that the second version of the Trust Agent software will also be available by the end of November. According to Cisco, the client software allows NAC systems to determine if security or management software such as Cisco's Security Agent software, or other required third-party antivirus software is correctly installed and up to date.

While Cisco's vision for NAC is one that eventually blends partnerships and standards to provide an open platform for heterogeneous, interoperable network security, currently NAC consists chiefly of Cisco technologies that work best in Cisco-only network infrastructures, and interoperability guarantees with leading client-side security-software vendors Trend Micro, Symantec and McAfee.

Figure 1.5: Security framework

Source: http://www.crn.com/security/172302008;jsessionid=1EO0W3J0JDRVQQSNDLPSKH0CJUNN2JVN

Based from the article in Figure 1.5 above, list down the action taken by Cisco in order to prevent their network from being attacked by malicious virus and intruder from outside. Share your findings in the LMS Forum.

1.5 TRENDS AND ISSUES IN COMPUTER SECURITY

The biggest revolution in security over the last 30 years has been the change in the computing environment from large mainframes to a highly interconnected network of much smaller systems. Security has switched from a closed environment or Local Area Network (LAN) to one in which computer can be accessed from almost anywhere or Wide Area Network (WAN/internet).

The type of individual who attacks a computer system or a network has also evolved over the last 30 years. The rise of non-affiliated intruders, including "script-kiddies," has greatly increased the number of individuals who probe organisations looking for vulnerabilities to exploit.

Another trend that has occurred is as the level of sophistication of attacks has increased, the level of knowledge necessary to exploit vulnerabilities has decreased (refer to Figure 1.6).

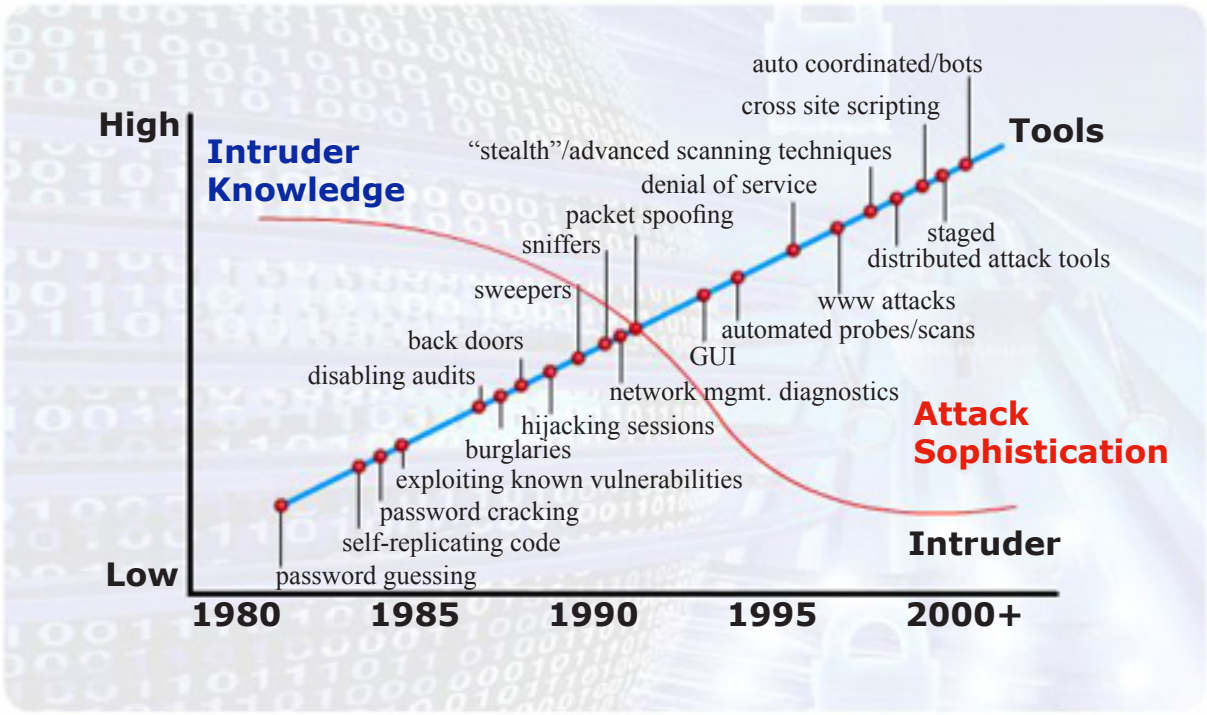

Figure 1.6: Security trends related to attack sophistication from www.cert.org
Source: http://www.cert.org

One of the best-known security surveys is the joint survey conducted annually by the Computer Security Institute (CSI) and the FBI.

The two most frequent and common types of attacks which are viruses and insider abuse of net access have remained constant.

- The number of organisations that have reported unauthorised use of their computer systems has been declining slowly (from 70% in 2000 to 56% in 2003).
- The number of organisations that have reported attacks from Internet connections has increased (from 59% in 2000 to 78% in 2003).
- Organisations citing independent hackers as a likely source of attacks have also increased (from 77% in 2000 to 82% in 2003).
- With the exception of Denial-of-Service attacks and telecom frauds, all categories had recorded a steady increase from 2000 through 2002, but then took a sharp decline in 2003.

The average loss as a result of theft of proprietary information hit a high of $6.57 million in 2002 but was only $2.70 million in 2003. Financial fraud plunged from $4.63 million in 2002 to $328 thousand in 2003.

SUMMARY

1. Computer security is a branch of technology known as information security as applied to computer(s).
2. It's generally related to Confidentiality, Integrity and Availability.
3. In order to implement the computer security, it is very important for organisations to properly develop and established their policies, procedures, standards and guide-lines to maintain the security of the systems and network.
4. In order for any IT security system to work, a well defined, organisation-wide security framework needs to be implemented that involves all stakeholders, and the framework needs to be part of the organisation's core operations at all levels of the organisational structure.
5. The trend that has occurred nowadays is that as the level of sophistication of attacks has increased, the level of knowledge necessary to exploit vulnerabilities has decreased.

GLOSSARY

Local Area Network (LAN)	A small typical local network covering a relatively small areas such as single floor of an office building.
Virus	A piece of malicious code that replicates by attaching itself to another piece of executable code.
Wide Area Network (WAN)	A computer network that spans a large geographic area, such as a network connecting offices in different cities.
Worm	A piece of code that attempts to propagate through penetration of networks and computer systems.

DISCUSSION QUESTION

Draft a security policy for protecting examination results kept on a computer system. Your policy should at least consider the access requirements of students, lecturers and administrator.

REFERENCES

Benson Yeung (2009). *The Security for Information Technology*. http://www.tns.com/it_security_framework.asp

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

Dieter Gollmann (2000). *Computer Security*. England: John Wiley & Sons.

Wm. Arthur Conklin, Gregory B.White & Chuck Cothren (2005). *Principles of Computer Security*. Singapore: Mc Graw Hill.