# CHAPTER 1

# INTRODUCTION

*"Raising awareness of information security for e-commerce and e-government is vital in this digital economy".*
*Chairman, Closing Speech, World Summit on the Information Society (WSOIS)[1],*
*Geneva, Switzerland, 10-12 December 2003.*

## 1. BACKGROUND OF THE STUDY

A few interesting things about information security to be food for thought:

- As opposed to other assets, information is something that can be stolen without being lost.
- As opposed to other assets, information is something that can be stolen without physical accessing.
- Yet, once it (confidentiality) is gone, it's gone forever.
- Like air, digital data (information) is intangible but in many cases, it's very costly if not critical to the survival of many companies or industries.
- Almost people protect their houses (even they possess nothing inside!) with lots of locks, fire extinguishers, alarms and bodyguards. Still, very few people do the same thing with their information asset. They seem to wait on a 'significant emotional event' to occur like the loss of customer credit cards or product information.
- Year by year, more and more time and efforts are spent on information security. Paradoxically, information assets seem to be more and more vulnerable.
- Only 22 countries in the world impose punishment on computer crimes (WSOIS Bulletin[1]).
- It took Bill Gates over ten years to become the richest man on earth and it might only need a day to make Microsoft go bankrupt once all the source codes of exclusive Windows operating system either were stolen or went public.
- Some viruses or worms such as 'I love you' or 'Code Red' need less than a week to be created but they can scatter throughout the world within an hour, causing a loss amounting up to hundreds of millions of US dollars.
- In 2002, US, Canada, UK, European Union, Japan, South Korea, Australia, Singapore and New Zealand spent approximately US$23 billion on information security whilst damages caused by viruses and attacks amounted up to US$32 billion (AFP News

Singapore[2]; AP News Belgium[3]; cited from Bangkok Post). As for Thailand, the overall security software market in 2003 would be worth US$11 million (Sasiwimon[4]).

- Among the world's top ten biggest IT issues of 2003, two go to information security – Spam mail and Internet attack. For sixth consecutive years, information security has become one of the primary concerns of not only the government but the industries as well (URL:http://www.infoworld.com/News[36]).

In this knowledge era, information is, undoubtedly, becoming an invaluable asset of enterprises. Due to that fact, there are more and more attacks on information, resulting in huge losses not only in finance but also in customers' loyalty. Based on statistics from PricewaterhouseCoopers (PWC), 71% of Thai companies and organizations have detected information security breaches and 47% of organizations here have been affected by viruses within the last 12 months. What's worth mentioning is that, according to Dr Viriya, a director at PWC Thailand, organizations here still lacked policy and serious efforts to update and maintain their systems. As an aftermath, security threats are on the rise (Karnjana[5]).

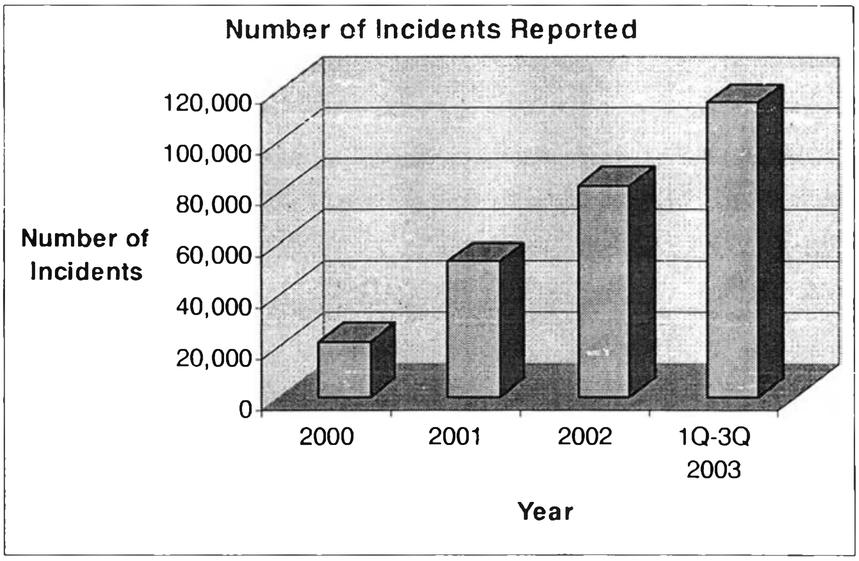


***FIGURE 1-1:*** *The number of incidents from 2000 to present (North America).*
***Source:*** *CERT/CC – URL:http://www.CERT.org/incidents[37];*

Additionally, as NECTEC's director Dr Thaweesak commented in his keynote address at the Government IT Week seminar, security is an important issue for every firm to be aware off, especially when firms are moving to offer their products and services online.

That comment is noteworthy. Traditionally, companies merely exploited the Internet as another channel to get closer to a wider audience (e.g. via advertising activities). Until recently, more organizations differentiate themselves by providing value-added services such as target marketing, customer relationship management (CRM), product lifecycle management (PLM), enterprise resource planning (ERP), payment aggregation and other innovative services. Thanks to network communication, organizations establish business relationships and transactions, say, supply chain and application service provisions. Unfortunately, such activities expose those organizations' information systems to countless vulnerabilities including computer-assisted fraud, espionage, sabotage, vandalism, malicious codes and programs (i.e. viruses, worms, Trojan-horses), denial of service (DoS) attacks and so forth. All these threats have, day by day, become more common, more ambitious and increasingly sophisticated.

Obviously, information, at each point of time, is of paramount importance to the survival or growth of every organization. Hence, the need to ensure business continuity as well as to minimize business damage or interruption by preventing, where possible, the consequences of information security breaches and incidents is understandable. In other words, the 'submarine warfare' against information security violations and incidents, which could come from anywhere at any time, is apparent and inevitable. Effectively and properly deploying levels of information security, we can enable information to be safely shared across networks meanwhile ensuring the protection of our mission-critical information and computing assets.

However much this information warfare may cost, we must spend as much time and effort as possible to protect our information assets. It is, simply, because we are living in the knowledge-based economy where information is power. Once we lose it, we lose everything.

*"The most noteworthy issue in information security management is, interestingly, never the technology itself. Rather, it is the issue of management as well as human-being."*
*Kevin D. Mitnick[6] – The world's most famous hacker*
*'The Art of Deception: Controlling the human element of security', 2003.*

*"Security is a management issue, not a technology issue".*
*Raymond R. Panko[7], Professor of Information System*
*University of Hawaii, Manoa.*

## 2. RATIONALE OF THE STUDY

Let's consider the following scenario. A network administrator at a manufacturing plant of electronics components thought that he had destroyed not only his employer's manufacturing capabilities but also the evidence that would link him to the crime. When he fell from the corporate grace and knew he was to be fired for performance and behavioral problems, he built a software time bomb to destroy the system.

Three weeks after this network administrator was fired, a plant worker started the day by logging on to the central file server. Instead of booting up, a message came on the screen saying an area of the operating system was being fixed. Then the server crashed, and in an instant, all of the plant's 1,000 tooling and manufacturing programs were gone. The server wouldn't come back up. The plant manager ordered that the manufacturing machines be kept running with the previous set of programs. He then was told that even the previous set of programs hadn't been filled.

Then the plant manager went to get his salvation – the backup disks, which are kept in a filing cabinet in the human resources department. Those disks were gone. He then turned to the workstations connected to the file server. The programs, at least a few of them, should have been stored locally on the individual workstations. Disappointedly, the programs weren't there.

The fired network administrator, the only employee responsible for maintaining, securing and backing up the file server, hadn't yet been replaced. In the day following the crash, the company called three people to attempt data recovery. Five days after the crash, the plant manager started shifting workers around the department and shutting down machines that were running out of raw materials or creating excess inventory. He took steps to hire a group of programmers to start rebuilding some of the 1,000 lost programs.

The plant's chief financial officer testified that the software bomb destroyed all the programs and code generators that allowed the company to manufacture 25,000 different products and customize those basic products into as many as 500,000 different designs. The company lost its twin advantages of being able to modify products easily and produce them inexpensively. It lost US$10 million, forfeited its position in the electronics industry and eventually had to lay off 80 employees.

That scenario was briefed from a real story of a manufacturing plant in Atlanta (Christopher and Audrey[8]). I wondered that such consequences wouldn't have happened should:

- there had been backup data and the site for backup data had been kept prudently in a secure place,
- the physical accesses to the central file servers and workstations had been strictly controlled,
- there had been at least two staffs being responsible for administering the network,
- disgruntled staff had been strictly supervised and most importantly,
- system audit had been carried out on a regular basis.

The answer is not what hard to find. It turned out to be that the trade-off for underestimating or overlooking information security is extremely costly.

In February 2000, web sites belonging to Yahoo, Buy.com, Amazon.com, CNN, ETrade and others were shut down for hours, the result of a massive coordinated attack launched simultaneously from thousands of different computers. Although most of the sites were back up within hours, the attacks were quite costly. Regardless of careful defense against such information security incidents, Yahoo, for instance, claimed to have lost more than a million dollars per minute in advertising revenue during the attack (Simson and Gene[9]).

As for Thailand, in October 2003, a European-owned bank's Internet banking service has been hacked, according to Advanced Certified Information Professional in Thailand (ACIS), director Prinya. The hackers had already successfully broken the SSL (Secure Socket Layer – It is simply a general-purpose protocol for sending encrypted information over the Internet) encryption and paid a visit to its customers' accounts (Sasiwimon[10]). Though the bank claimed to have lost nothing, there was a heighten fear among their shareholders as well as customers. This worry is, in my opinion, reasonable since, equipped with the highest security level, the bank cannot be exempted from unauthorized intrusions. Certainly, this kind of reported security information breach is not rare. However, many more violations and incidents are uninformed, unidentified or untestified, according to Dr.Komain – director of Thai Computer Emergency Response Team (ThaiCERT) – due to confidentiality and customers' credit damage.

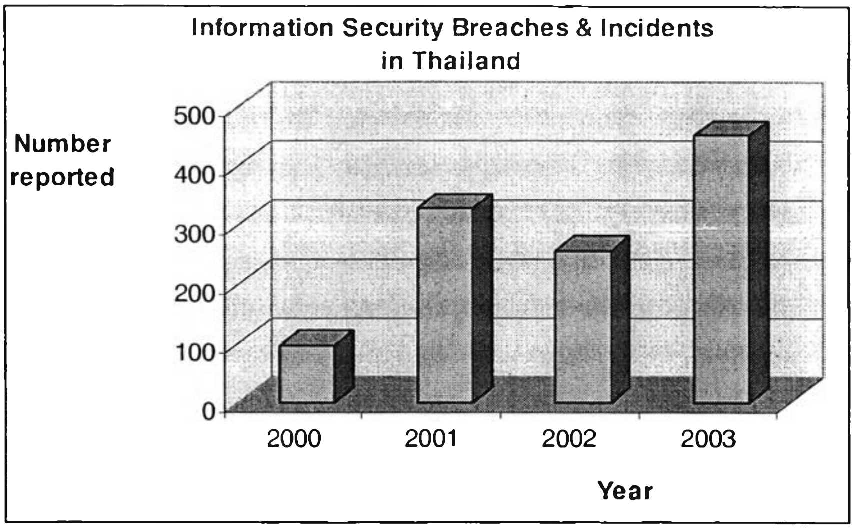


***FIGURE 1-2:*** *The number of incidents in Thailand from 2000 to present*
***Source:*** *Dr.Komain, Head of ThaiCERT[63] – A division of NECTEC, January 2004 .*

Not only are such attacks limited to banks, companies or manufacturing plants. Suprisingly, according to Richard Power, editorial editor for the Computer Security Institute, it's the universities that make very good targets for attack. As explained by Richard, little monitoring or management, lack of training on security measures, free exchange of ideas and loosely-controlled access, to name but a few, are factors that attribute to information security violations and incidents (cited from Charles and Shari[11]). Many prestigious US universities such as Stanford University, MIT, Yale and Princeton used to be the victims.

For example, on 5 June 2003, Stanford's network is being severely impacted by a Windows-based virus (URL:http://www.standford.edu/itss/news[38]). Spreading through email system, the virus sent out copies of randomly-selected files from victim machines, some of which may contain sensitive information such as salary and bonus spreadsheets, personal data, and other highly confidential files. Worse yet, the virus disabled anti-virus and personal firewall software, installed a program which allows remote users to view files and started processes on infected machines and included a keystroke logger which can record passwords and other confidential information. Due to this severe consequence, many services on the campus network were shut down, affecting communication activities of thousands students and staff. Similar but more intense information security breaches can be found at M.I.T (URL:http://www.mit.edu/cpnews[39]). Yale University (URL:http://www.aba-dialogue.org; cited from Pamela and Michael[12]) and Princeton University (URL:http://dailynews.muzi.com/ll/english/1219068.shtml, cited from Pamela and Michael[13]). Back to the above-mentioned attack on Yahoo, Buy.com, Amazon.com, CNN, Etrade, Mr.David – a security engineer at the University of Washington – confirmed that those who performed the sabotage must have practiced on the university network (cited from Charles and Shari[11]). Those figures and facts cannot fail to make us jump out of our skin.

Things still hold true in Thailand. As far as the digital attacks are concerned, according to the Internet thermometer (URL:http://www.zone-h.org[40]), government and academic institutes here are the most attacked websites. For these organizations, losses and damages, if occurred, are immeasurable since they regards national security, academic and research activities and many other systems.

The list of damaged organizations could go on.

In recent years, owing to an exponential increasing of information security violations and incidents, there have been numerous systems, tools and techniques including hardware and software, standards, best practices and strategy deployed by many organizations. Sadly still, few of them are quite successful.

This, personally, could be preliminarily explained as followed:

- The most important issue in dealing with information security, in my opinion, does not lie entirely in the system, tools or techniques themselves to implement. Rather, it lies in the way the organizations manage their risks. In other words, choosing an appropriate approach to assess and correctly performing risk assessment are equally significant. Only then can we identify which are the organization's risks, where they come from, how they occur and most importantly, what are the organization's losses upon their occurrence.
- The other issue is, certainly, the information security management system or techniques to deploy. As far as the effectiveness of those systems or techniques is concerned, the systems or tools themselves must reveal their positive effects on those identified risks, whereby ensuring business continuity and minimizing business losses the organization might encounter. In order to do so, it is crucial that the selected systems and techniques must be of a wide range of concerning areas, up-to-date and well designed.

The two reasons mentioned above are also the rationale of this study.

## 3. THESIS OBJECTIVE & RESEARCH QUESTIONS

Given the above rationale, I would choose the Engineering Computer Center (ECC) at the Faculty of Engineering as a specific case to establish an Information Security Management System (ISMS) mainly based on Information Security Management Standards - ISO 17799:2000 and BS 7799-2:2002.

More concretely speaking, the objectives of this thesis work are:

- Study the threats, vulnerabilities and impacts from a perspective of information security by conducting a risk assessment via using the OCTAVE$^{SM}$ method developed by CERT/CC (Computer Emergency Response Team/Coordination Center) at the Software Engineering Institute (SEI), Carnegie Mellon University.
- Based on the outcome of this evaluation, an efficient Information Security Management System (ISMS) will be developed for ECC. This establishment of ISMS is mostly based on the Information Security Management Standards (ISMS) - BS 7799:2-2002 and ISO/IEC 17799:2000 and other available internationally recognized documents.

In order to fulfill these objectives, some questions should be taken into accounts:

1. What is an ISMS and why to develop it?
2. Which approach will be used to conduct risk assessment? Why?
3. Which are the ECC's information security threats and vulnerabilities?
4. How and where do those threats come from?
5. What are the consequences of those threats?
6. What are the impacts on the ECC? What are ECC's threat profiles?
7. Which ISMS model will be adopted? Why?
8. How to develop an efficient ISMS? What are the components of an ISMS based on ISO 17799:2000 and BS 7799-2:2002?
9. What needs to be taken into consideration before and after the establishment of this ISMS?

## 4. SCOPE

Describing the whole subject of ISMS (i.e. establishing, maintaining, etc.) would, in many times, extend the volume of this thesis work. Thus, some limitations should be done.

First of all, this work is going theoretical. It means that the study focuses only on establishing the ISMS. It is important because meeting all conditions and steps for both establishing and maintaing ISMS (i.e. in terms of practice), as described in BS 7799-2: 2002, would require a large amount of thesis work. But yet, as great as the establishment of an ISMS is concerned, I will develop a complete Information Security Management System (ISMS) by intimately presenting all steps as well as processes mentioned in the standard so that readers will have a better visualization of what the ISMS will look like in practice. Controls from the standard, accompanied by additional safeguards from other internationally recognized resources, will be selected in accordance with the risk assessment results.

Secondly, regarding the risk assessment method, I will focus only on the OCTAVE$^{SM}$ method developed by CERT/CC (Computer Emergency Response Team/Coordination Center) at the Software Engineering Institute (SEI), Carnegie Mellon University. Whilst there are abundant sources of risk assessment method, the one developed by Carnegie Mellon University appears to be dominant because of two reasons. First, in this method, many points in the catalog of practices are adapted from the BS 7799-1:1995 – the former of the latest BS 7799-2:2002 that is currently internationally recognized. Second, the OCTAVE$^{SM}$ method reveals the flexibility that is quite convenient to modify into each specific context. More benefits as well as advantages of selecting this method will be presented hereafter.

The last limitation is that I will mostly focus on the ISMS - BS 7799 and ISO/IEC 17799. There have, so far, been a few ways of establishing an ISMS. Though the standards like "The Orange Book – Information Security Management Manual" or "ITSEC" are in common use, it is tempting that only BS 7799 and ISO/IEC 17799 would be the main theme. There are a few reasons for it. First, this standard gets more and more users and becomes the most widely accepted and recognized (Vigilinx[14]; Karnjana[5]). In effect, BS regulation was so popular that within over one year ISO decided to spread the standard worldwide. As a result, ISO standards were adapted from the original BS 7799:1-1999 standard to become the new ISO/IEC 17799:2000 – the only standard for Information Security Management (ISO 17799: 2000). Second, in the near future, it can possibly end up as a consistent part in an integrated ISO set of collection (e.g. together with ISO 9000:2000) like it used to be with triangle ISO 9001 + ISO 14001 + ISO 18001 (Szomanski[16]). And third, according to Karnjana[5], the National Security Council (NSC) would publicly announce the enforcement of the standard for all royal governmental agencies, companies and academic institutions. As such, preparation for this ISMS is crucial and just a matter of time.

## 5. METHODOLOGY

This study is expected to be carried out in the following steps:

1. Do a literature research on both traditional paper-based documents as well as online database.
2. Collect data and study the previously implemented models, available risk assessment, best practice, techniques, policy and strategy.
3. Conduct a survey on ECC's organizational structure as well as its operation.
4. Conduct information security risk assessment using OCTAVE$^{SM}$ method.
5. Analyze the identified risks and threats of ECC's information system.
6. Establish an ISMS by properly using BS 7799-2:2002, ISO/IEC 17799:2000 and other available recognized sources.
7. Summarize and recommend further studies.

## 6. EXPECTED RESULTS

At the end of this study, there will be two expected results that are aligned with the above stated objectives:

- Clearly identify what are the threats, vulnerabilities, outcomes and impacts that might affect the ECC's information system. Threat profiles from risk assessment will be of utmost significance not only for the establishing ISMS later in this thesis but for further research hereafter as well.
- Given the threat profiles, describe an ISMS that can effectively protect the system from those risks and ensure operational continuity. An ISMS would also be significant for further reference in the future.

## 7. AN OUTLINE OF THIS THESIS WORK

Logically speaking, this thesis work is divided into five chapters as followed:

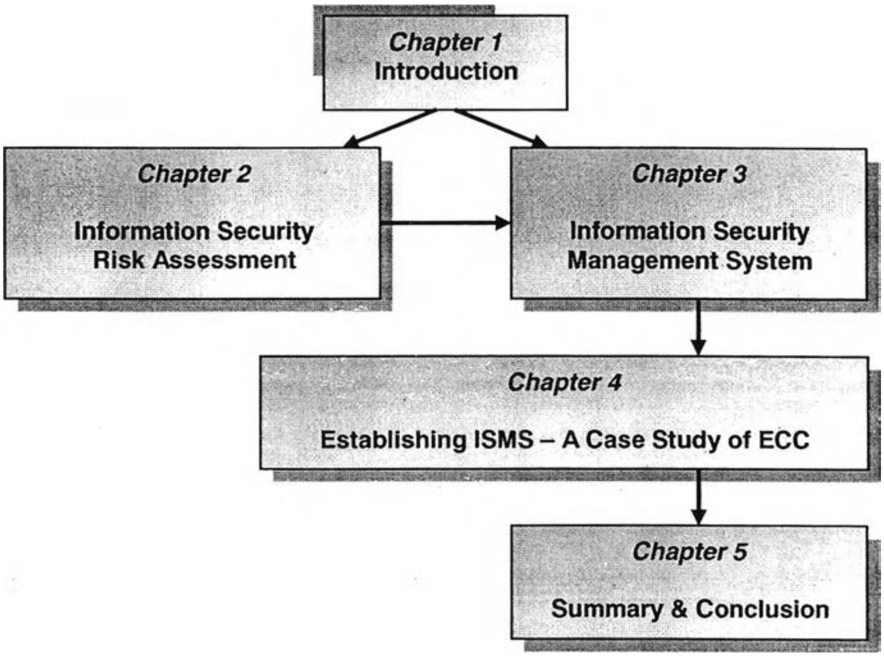
- *Chapter 1 - Introduction:* This chapter will provide the readers with an overview of what will be discussed and analyzed throughout the study. Readers will have a thorough grasp of the background and rationale of the study. Some typical examples, figures and well-known illustrations are presented to highlight the panorama. Next, the identified problems will be transformed into the objectives and research questions, which will drive the contents of this research. Finally, chapter 1 will be closed with the scope, methodology and expected results that give the readers the expected destination.

- *Chapter 2 – Information Security Risk Assessment:* Risk assessment – an indispensable and vital element of managing information security risks – is intimately mentioned in this chapter. The chapter will start with some basic definitions such as information, information security requirements, and risk assessment methodology. What's more, there go some popular approaches to risk assessment whose origins, characteristics and methodologies are preliminarily introduced. Among those approaches, OCTAVE$^{SM}$ method is deeply presented so that the readers can understand its advantages and methodologies. Lastly, readers will have a glance at some of the computer-aided-risk-assessment tools available in the market, which are of great help to do a large amount of work at large, complex organizations.

- *Chapter 3 – Developing an Information Security Management System (ISMS):* Readers now arrive at one of the main contents of this study. The chapter starts with basic concepts such as definitions of ISMS and a glance at its history. Then, some practical approaches to modern ISMS in the industry are presented and analyzed. After having an overall view of those models, ISO 17799 and BS 7799 will be deeply discussed so that readers understand their importance and content. Finally, in relation to those standards, an in-depth into the ISMS will be given.

- *Chapter 4 – Engineering Computer Center (ECC) & its ISMS:* All of the above-mentioned theories are now materialized for a real case of ECC. There are two main themes in this presentation. First, risk assessment will be tapped in terms of details of the whole processes conducted and results obtained. Second, steps to fully establish an ISMS are presented in accordance with the selected framework of chapter 3.

- *Chapter 5 – Summary & Conclusion:* This final chapter will end the study with some answers for research questions (in section 3, Chapter 1) regarding theories, practices, tools, techniques and models applied. A few highlighted points will be recalled so that the readers, even without reading the above chapters, may have somewhat understanding about what is going throughout the presentation. Then, a conclusion will give the readers some lessons from the study and suggestions for future study.


Chapter 1
Introduction
Chapter 2
Information Security Risk Assessment
Chapter 3
Information Security Management System
Chapter 4
Establishing ISMS – A Case Study of ECC
Chapter 5
Summary & Conclusion