Briefing Note 6

January 2010

Network and Information Security and Privacy

United Nations Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT)

APCICT Briefing Note No. 6
Network and Information Security and Privacy

Summary

In today's society, governments, public institutions and private corporations collects, processes and stores confidential information about their employees, customers, products, research and financial status in electronic format, which can be transmitted globally across networks. Information is an asset to be protected and policymakers need to know what information security is and how to take action against unauthorized access, use, disclosure, disruption, modification or destruction. This briefing note provides an overview of the need for information security, information security issues and trends, and the process of formulating an information security policy.

This briefing note is drawn from the sixth of nine core modules of the Academy of ICT Essentials for Government Leaders (Academy). The Academy is a comprehensive ICT for development training curriculum that aims to equip policymakers with the essential knowledge and skills to fully leverage opportunities presented by ICT to achieve national development goals and bridge the digital divide. More information on the Academy is available at http://www.unapcict.org/academy.

Author: Freddy Tan

Series Editor: Christine Apikul

1. Introduction

In today's information society, where information has become a valuable asset and where the advancement of technologies and people's dependence on them have enabled easier access to information, this makes individuals, organizations and nations highly vulnerable to information security attacks.

Threats to the Internet first began in the 1980s with the advent of 'hackers' and malware developers who seek to produce damage with the intent of looking for notoriety or causing havoc. Macro and script viruses saw faster propagation leveraging the Internet. However, in the 21st century, we began to witness Spamming, Phishing and Botnets, where capital is the motivator.

2. Types of Information Security Threats

The range of threats to information and communication technologies (ICTs) is vast — from consumer threats (e.g., becoming a 'bot', theft of personally identifiable information, and child endangerment), to enterprise threats (e.g., theft of intellectual property, customer information), to national threats (e.g., espionage, denial of service attacks).

At the same time, there is increasing concern about social aspects in the digital age. Some of this concern is a function of the criminal landscape, like the theft and misuse of personal credentials. But increasingly, there are concerns over child sexual exploitation, Internet addiction, online pornography, privacy and other social issues that are far broader than just public safety concerns. Through social networking applications, individuals today generate far more information in our electronic lives and how that data can be collected, aggregated, analysed, disseminated, and used is becoming an important issue.

3. Information Security Methodology

In the Information Age, information is an asset to be protected and policymakers need to know what information security is and how to take action to protect information and intellectual property from leakage and infringement. Policymakers need to recognize the key considerations for information security issues and trends, and the process of formulating an information security strategy.

However, security is not an end state. Security threats will continue to evolve with technology.

As such, much akin to how we deal with automobile, aviation and shipping risks such as accidental collisions, hijacks and loss of assets, we need a combination of regulations, technological standards and competencies to protect individuals, organizations and nations from threats to ICT, such as computer hacking, cyberterrorism, cybercrime, and the like.

And like the automobile, aviation and shipping industries, governments have an important role to play in ensuring information security by expanding the information-communication infrastructure and establishing systems to protect against ICT threats.

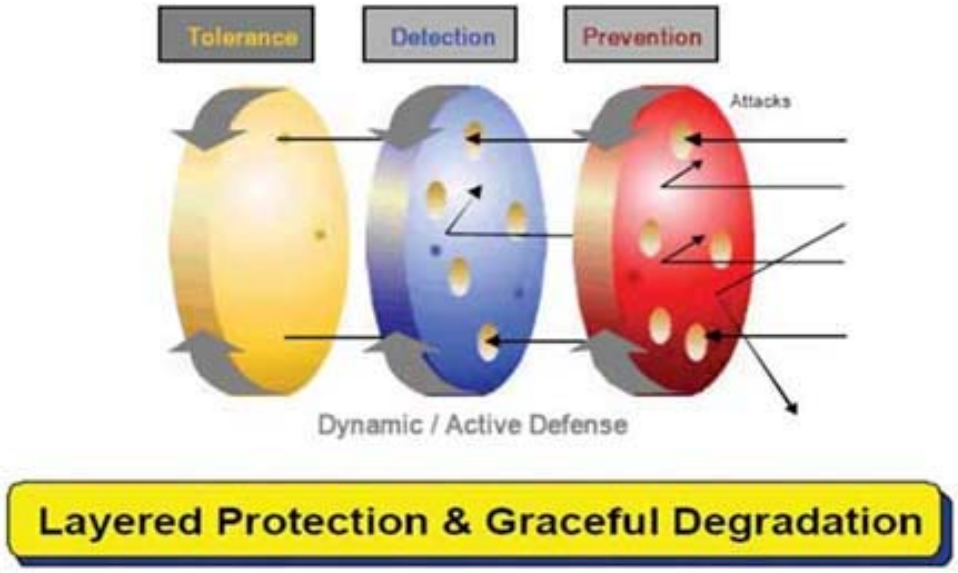

Figure 1 Defense In Depth

It is important to note that various security technologies have been developed to help organizations secure ICT. However, it must be recognized that such technologies are not fool-proof due to human errors, inherent unknown system vulnerabilities, administrative lapses, available resources and technical competencies.

As such, today's security systems need to be deployed based on a Defense-In-Depth (DID) model that leads to unified management of the technologies involved. This model is different from perimeter defense, which has only one layer of defense against all threats. The DID model consists of prevention, detection and tolerance, with threats being mitigated at each phase.

4. Information Security Policy Considerations

In defining a national information security policy framework, policymakers need to take into account a number of considerations, among them the rationale for a policy, available resources, the policy direction, budgetary and legal requirements, and expected policy outcomes. In addition, the national information security policy should include the information security strategy, legal relationships, information security organization, information security technology, and the interrelationships among them.

Three important attributes that policymakers need to recognize are:

1. Know the threat landscape
2. Keep abreast with vulnerabilities in ICT
3. Know the value/liability of information on ICT

Policymakers must ensure that the available resources are directed at protecting the ICT against the threats, that known vulnerabilities are addressed and that information risks are managed adequately. Policymakers need to collaborate with the academia and private industry to ensure that a vibrant security ecosystem is developed. Technology is only as good as the people who manage the technology.

Policymakers today can draw on the experience and work of many international, regional, national and industry in the area of information security activities and in implementing a national information security policy. These include countries of the European Union (EU), Germany, Japan, Republic of Korea, Singapore and the US, and international organizations like the Asia-Pacific Economic Cooperation, International Organization for Standardization and International Electrotechnical Commission, International Telecommunication Union (ITU) and Organisation for Economic Co-operation and Development.

There are also many initiatives that have gained popularity and adoption. One example is the Council of Europe Convention on Cybercrime (CECC), promulgated in 2001, which "lays down guidelines for all governments wishing to develop legislation against cybercrime" and "provides a framework for international co-operation in this field." Thirty-nine European countries signed the treaty, as well as Canada, Japan, South Africa and the US. This makes the CECC, which entered into force in July 2004, "the only binding international treaty on the subject to have been effectuated to date."

It should however, be noted that different countries will have slightly different policy considerations and contexts.

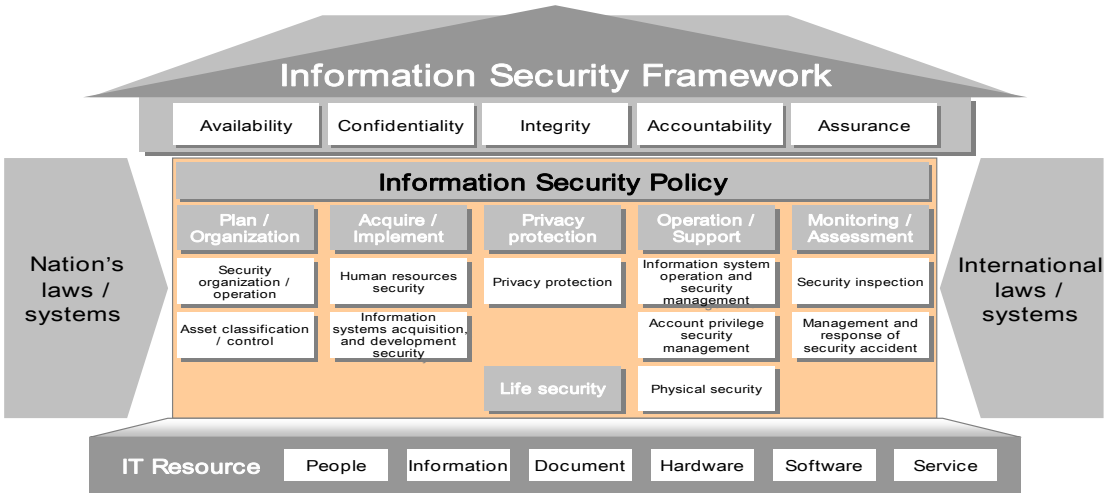

Figure 2. Information Security Framework

Responding effectively to threats and information security violations requires cooperation among the national information organization, investigative agencies and legal institutions, as well as organizations that conduct security accident inspection and damage estimation. It is also essential to cooperate with organization that can analyse technical vulnerabilities and prescribe technical countermeasures.

Due to the global nature of the Internet, policymakers must recognize that information security cannot be achieved through the efforts of one country alone because information security violations tend to be cross-border in practice. Thus, international coordination in information security protection, both in government and in the private sector, must be institutionalized.

For the private sector, the relevant international organization for the promotion and protection of information security is the Computer Emergency Response Team

Coordination Center. Among governments, the European Network and Information Security Agency (for the EU) and the ITU aim to foster cooperation in information security among countries. In each country there must be a government institution whose role is to facilitate cooperation by both government and private organizations with international agencies and institutions.

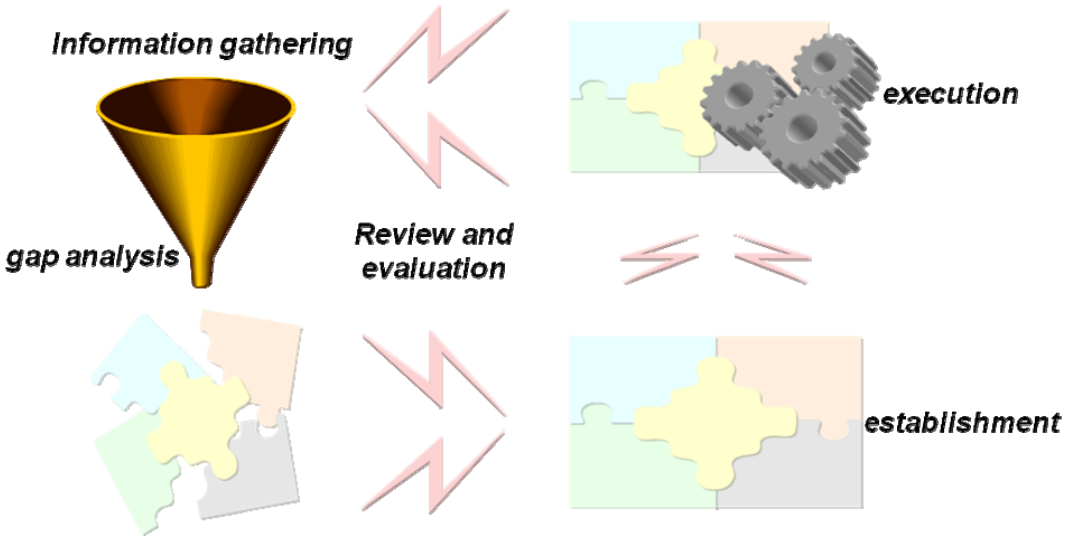

Figure 3. Life Cycle of Information Security Policy

Lastly, information security policy life cycle is a continuous process that can be broadly divided into four phases (see Figure 3):

1. Information gathering and gap analysis
2. Establishment of the policy
3. Implementation of the policy
4. Control and feedback

Information security policymakers need to continually review the national security policy and supplement underdeveloped areas. Policy revision is also essential to measure the efficiency of an information security policy.

However, there remain challenges as a result of the way the Internet was designed and managed, and the exponential growth of the digitally wired society. These issues will remain whilst international organizations, national governments and the industry collaborate to find a better way to address them. The issues include:

- Global connectivity
- Anonymity
- Lack of traceability and trust
- Increasing valuable targets

The **APCICT Briefing Note Series** aims to provide at-a-glance information on key information and communication technology for development (ICTD) agendas for high-level policymakers and stakeholders. The series includes: 1) highlights of conventional research papers, assessment and survey reports and publications; 2) policy considerations drawn from the Academy modules; and 3) key challenges and lessons learned based on analyses of best practices and case studies.

APCICT, a regional institute of the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP), was established and inaugurated on 16 June 2006 in Incheon, Republic of Korea. The role and mission of APCICT is to strengthen the efforts of the 62 ESCAP member and associate member countries to use ICTs in their socio-economic development through building the human and institutional capacity for ICT. In pursuance of this mandate, APCICT's work is focused on three inter-related pillars – Training, Advisory Services and Research. The Briefing Note Series is part of the research pillar. Also under the research pillar is a Case Study Series that provides analyses and compilations of best practices and case studies on different aspects of ICTD and capacity building in the Asia Pacific region.

Contact information:

United Nations Asian and Pacific Training Centre for Information and Communication Technology for Development (UN-APCICT)

Bonbudong, 3rd Floor Songdo Techno Park
7-50 Songdo-dong, Yeonsu-gu, Incheon City
Republic of Korea

Telephone: +82 32 245 1700-02
Fax: +82 32 245 7712
E-mail: info@unapcict.org

http://www.unapcict.org