Information Security and Privacy

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

Summary

In today's society, governments, public institutions, and private corporations collect, process, and store 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 of information. 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 module of the Academy of ICT Essentials for Government Leaders (Academy). The Academy is a comprehen-nsive information and communications technology (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: Korea Internet and Security Agency

Module 6 - Information Security and Privacy
Presents information security issues and trends, and the process of formulating an information security strategy.

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.

Participants observing presentation on Information and Security and Privacy at the second UN-APCICT/ESCAP Training of Trainers (TOT) Workshop in Seongnam, Republic of Korea (March 2009)

1 Introduction

In today's information society, information has become a valuable asset and there is increasing dependence on 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 emergence of 'hackers' and malware developers who were motivated by the desire for notoriety as well as the thrill of wreaking havoc. Using the Internet, they were able to quickly propagate macro and script viruses. In the 21st century, spamming, phishing, and botnets are the new information security threats, and their perpetrators are motivated by the desire for profit.

2 Types of Information Security Threats

Threats to information and communications technologies (ICTs) range from consumer threats (e.g. becoming a 'bot', theft of personally identifiable information, phishing and child endangerment), to enterprise threats (e.g. theft of intellectual property and customer information), to national threats (e.g. espionage, denial of service attacks and advanced persistent threat).

At the same time, there is increasing concern about social aspects in the digital age.

"Mr. Grimshawe, somebody's hacked into the office computer!"

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 public safety concerns. Through social networking applications, individuals today generate greater amounts of information electronically, and how that data can be collected, aggregated, analysed, disseminated, and used are 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 information security issues and trends, and understand the process of formulating an information security strategy.

An important point to consider is that security is not an end state. Security threats will continue to evolve with technology. Thus, in the same way that 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, cyber terrorism, cybercrime, and the like.

And as in 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.

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. 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.

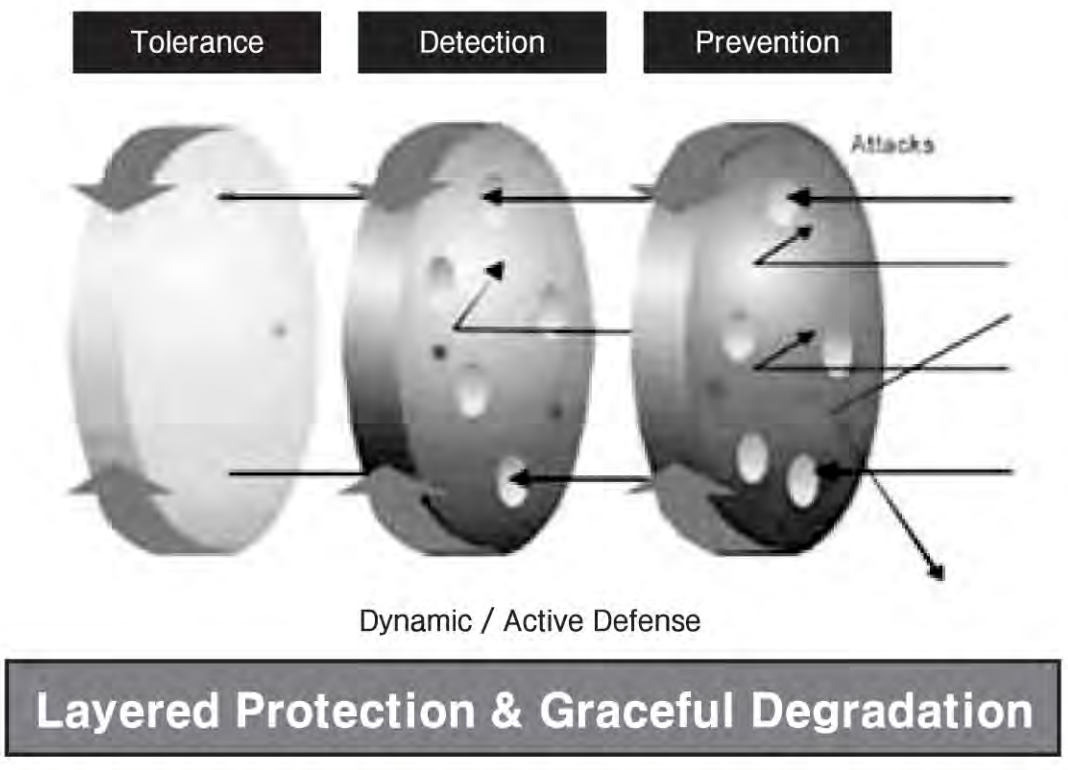

Figure 1: Defense in Depth
Module 6: Network and Information Security and Privacy, p. 32
(Source: Defense Science Board, Protecting the Homeland: Defensive Information Operations 2000 Summer Study Volume II, Washington, D.C.: Defense Science Board, 2001, 5, http://www.acq.osd.mil/dsb/reports/dio.pdf)

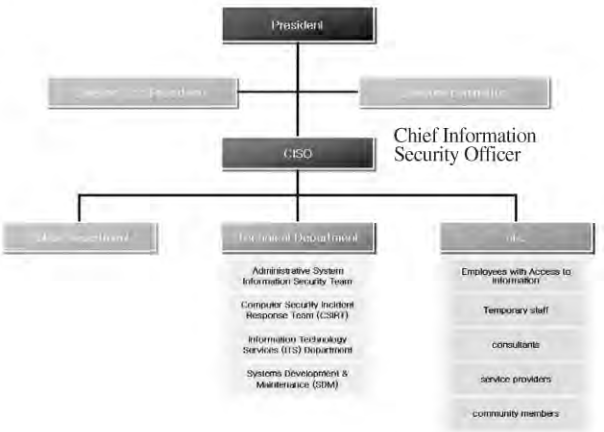

Figure 2. Sample national information security organization
Module 6: Network and Information Security and Privacy, p. 91

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.

Policymakers should have the ability to:
1. Know the threat landscape.
2. Keep abreast of vulnerabilities in ICT.
3. Determine the value and liability of information on ICT.

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

Group discussion on Network and Information Security and Privacy at the second UN-APCICT/ESCAP Training of Trainers (TOT) Workshop in Seongnam, Republic of Korea (March 2009)

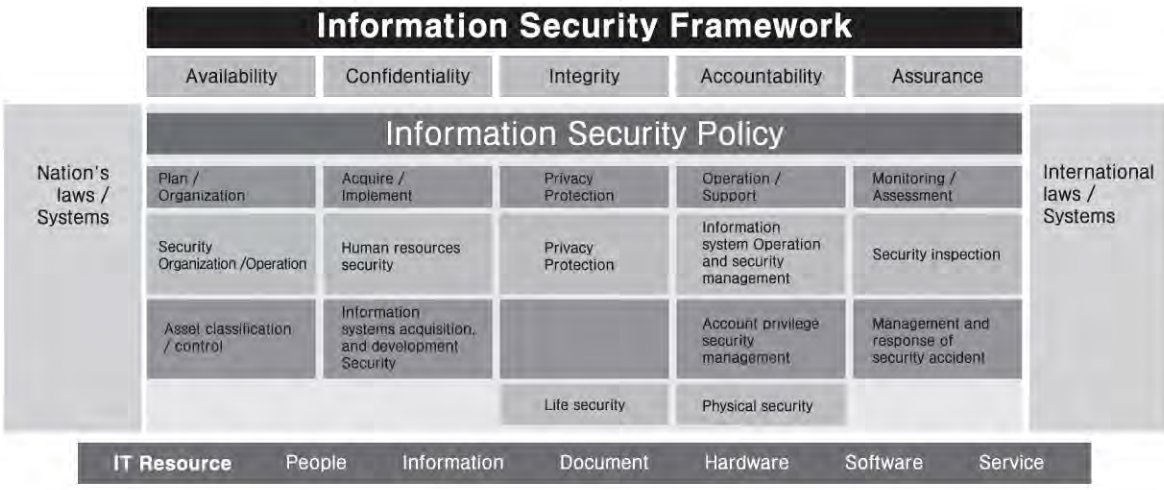

Figure 3: Information Security Framework
Module 6: Network and Information Security and Privacy, p. 93

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

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.

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 organizations that can analyze 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 the government and 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. (CERT/CC) 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

Figure 4. Areas for cooperation in information security policy implementation
Module 6: Network and Information Security and Privacy, p. 99

Lastly, information security policy life cycle is continuous. It consists of four phases that are cyclical (see Figure 5):

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.

Figure 5. Life Cycle of Information Security Policy
Module 6: Network and Information Security and Privacy p. 87

Because of the way the Internet is designed and managed, and the exponential growth of the digitally wired society, new challenges to information security are constantly emerging. International organizations, national governments, and the industry need to collaborate to find a better way to address these challenges, which include:

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

National workshop of the "Academy of ICT Essentials for Government Leaders" on Network and Information Security and Privacy, co-organized by the Indonesian Ministry of Communication and Information Technology and University of Indonesia in collaboration with the UN-APCICT/ESCAP in Solo, Indonesia. (July 2009)

UN- APCICT / ESCAP

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.
http://www.unapcict.org

ESCAP

ESCAP is the regional development arm of the United Nations and serves as the main economic and social development centre for the United Nations in Asia and the Pacific. Its mandate is to foster cooperation between its 53 members and 9 associate members. ESCAP provides the strategic link between global and country-level programmes and issues. It supports Governments of countries in the region in consolidating regional positions and advocates regional approaches to meeting the region's unique socio-economic challenges in a globalizing world. The ESCAP office is located at Bangkok, Thailand.
http://www.unescap.org

The Academy of ICT Essentials for Government Leaders

(http://www.unapcict.org/academy)

The Academy is a comprehensive ICT for development training curriculum with eight initial modules that aims to equip policymakers with the essential knowledge and skills to fully leverage opportunities presented by ICTs to achieve national development goals and bridge the digital divide.

Module 1 - The Linkage between ICT Applications and Meaningful Development
Highlights key issues and decision points, from policy to implementation, in the use of ICTs for achieving the Millennium Development Goals.

Module 2 - ICT for Development Policy, Process and Governance
Focuses on ICTD policymaking and governance, and provides critical information about aspects of national policies, strategies and frameworks that promote ICTD.

Module 3 - e-Government Applications
Examines e-government concepts, principles and types of applications. It also discusses how an e-government system is built and identifies design considerations.

Module 4 - ICT Trends for Government Leaders
Provides insights into current trends in ICT and its future directions. It also looks at key technical and policy considerations when making decisions for ICTD.

Module 5 - Internet Governance
Discusses the ongoing development of international policies and procedures that govern the use and operation of the Internet.

Module 6 - Information Security and Privacy
Presents information security issues and trends, and the process of formulating an information security strategy.

Module 7 - ICT Project Management in Theory and Practice
Introduces project management concepts that are relevant to ICTD projects, including the methods, processes and project management disciplines commonly used.

Module 8 - Options for Funding ICT for Development
Explores funding options for ICTD and e-government projects. Public-private partnerships are highlighted as a particularly useful funding option in developing countries.

Module 9 - ICT for Disaster Risk Management

Module 10 - Climate change and ICT (to be launched in 2012)

APCICT Virtual Academy

(http://e-learning.unapcict.org)

- An online distance learning platform that brings Academy training to a wider audience.

Knolwedge Management

- **e-Collaborative Hub** (e-Co Hub - http://www.unapcict.org/ecohub); A resources portal and knowledge sharing network for ICTD.

- **Digital Partnership Network** (DPN - http://www.unapcict.org/join_form); A collaborative ICTD network of academics, development practitioners and policymakers.

Research for ICT Human Capacity Building

- Analytical studies and cutting-edge research on ICTD and ICT human capacity building to provide support for making appropriate decisions on ICT policies and sharing of best practices.

Advisory Services

- Advice and support to partners for design, customization, localization and roll out of ICTD capacity building programmes.

Turning Today's Youth into Tomorrow's Leaders Programme

- Investing in and training the region's future leaders and workforce to develop sustainable ICT capacity.

This work is released under the Creative Commons Attribution 3.0 License.
To view a copy of this license, visit http://creativecommons.org/licenses/by/3.0/

The opinions, figures and estimates set forth in this publication are the responsibility of the authors, and should not necessarily be considered as reflecting the views or carrying the endorsement of the United Nations.

The designations used and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Mention of firm names and commercial products does not imply the endorsement of the United Nations.