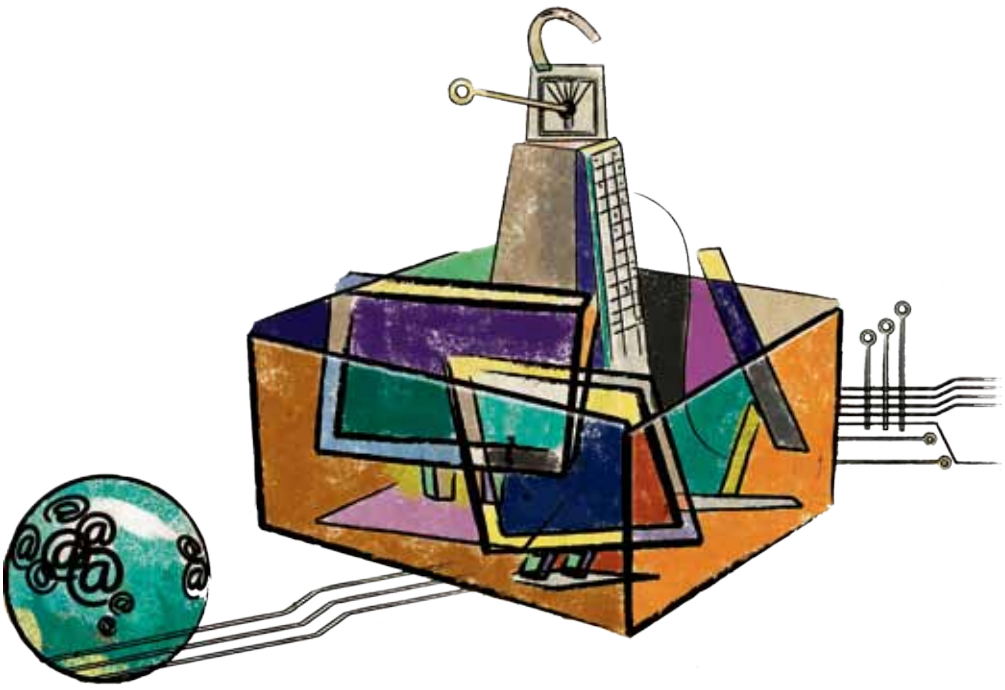
KNOWLEDGE SHARING SERIES

ISSUE II

CYBERSECURITY



UNITED NATIONS ESCAP
Economic and Social Commission for Asia and the Pacific
/APCICT

MINISTRY OF STRATEGY AND FINANCE
REPUBLIC OF KOREA

Knowledge Sharing Series

Issue 2

Cybersecurity

Heung Youl YOUM
Euisun PAIK

APCICT **ASIAN AND PACIFIC TRAINING CENTRE FOR INFORMATION AND COMMUNICATION TECHNOLOGY FOR DEVELOPMENT**

Knowledge Sharing Series

Issue 2: Cybersecurity

Contact:
United Nations Asian and Pacific Training Centre for Information
and Communication Technology for Development (UN-APCICT/ESCAP)
Bonbudong, 3rd Floor Songdo Techno Park
7-50 Songdo-dong, Yeonsu-gu, Incheon City
Republic of Korea

Tel: 82 32 245 1700-02
Fax: 82 32 245 7712
E-mail: info@unapcict.org
http://www.unapcict.org

ISBN: 978-89-959820-1-3

Cover Designer: Min Chong Koh
Design and Layout: Scand-Media Corp., Ltd.
Printed in: Republic of Korea

Supported by

MINISTRY OF STRATEGY AND FINANCE
REPUBLIC OF KOREA

Korea Eximbank

Coordinated by

KDS Korea Institute for Development Strategy

FOREWORD

The transformational power of information and communication technologies (ICTs) in connecting people, improving business efficiency and empowering communities — eliminates any doubt about the importance of making these technologies accessible to all and ensuring that everyone has the capacity to harness their potential.

The 'mobile miracle' has brought the benefits of ICTs within reach of nearly everyone. In less than five years, the number of mobile phone subscriptions in Asia and the Pacific more than doubled, rising from 1.08 billion to 2.53 billion.[1]

As we know however, ICT is not only about connectivity. More importantly, it is about leveraging the power of connected technologies for inclusive and sustainable development. Two decades ago, phones were used, almost exclusively, for talking to one another. Presently, a wide range of services and applications are available on mobile phones that are being used every day for banking, learning, and obtaining real-time information - helping to improve people's lives.

However, the benefits of ICTs are still not available to everyone. In fact, the digital divide in Asia and the Pacific is one of the widest in the world. For instance, the least developed Asia-Pacific countries and the Pacific island developing economies have, on average, fewer than 28 mobile phone subscriptions per 100 persons, compared to an average of 99 in high-income countries. A similar pattern can be found in Internet usage with 1 per 100 in least developed countries, compared to 78 per 100 in high-income countries.[2]

Without adequate access and capacity to utilize ICTs, least developed countries and marginalized populations risk falling further behind the rest of the world and will face great difficulties catching up, thus widening the digital divide.

Much remains to be done to ensure inclusive and sustainable Asia-Pacific growth. Unfortunately, the growth of ICT availability has not been matched by an equally rapid expansion in knowledge concerning the opportunities and challenges that ICTs present, and the ways to effectively leverage the potential of ICTs for development.
To bridge this knowledge gap, the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP) welcomes the launch of the Knowledge Sharing Series being spearheaded by the Asian and Pacific Training Centre for Information and Communication Technology for Development (UN-APCICT/ESCAP), one of our ESCAP regional institutes.

As ICT for development (ICTD) programmes are often huge undertakings, that cut across multiple sectors, and require the participation of stakeholders from multiple specializations, knowledge sharing is fundamental to the effective development and implementation of ICTD strategies and plans, to the creation of innovative ICT solutions to complex development challenges, and to the avoidance of pitfalls and duplication of efforts. Knowledge sharing is, in fact, an important component of lifelong learning and capacity building, as it promotes a better and deeper understanding of different aspects of ICTD from various perspectives. Knowledge sharing is also a catalyst for establishing partnerships. This Knowledge Sharing Series has been developed for precisely these reasons.

As our member States continue to grapple with the effects of global economic uncertainty, ICT as an enabler for development, has become a key element in national strategies for building social and economic resilience, and promoting inclusive and sustainable development. It is therefore more important than ever to share ICTD knowledge to develop synergies, pool resources and strengthen capacities for shaping a safer and more sustainable future.

Noeleen Heyzer

Under-Secretary-General of the United Nations
and Executive Secretary of ESCAP

1 http://wwwupdate.un.org/wcm/content/site/chronicle/cache/bypass/home/archive/thedigitaldividend/digitalasiapacificinthe21stcentury?ctnscroll_articleContainerList=1_0&ctnlistpagination_articleContainerList=true

2 http://www.unescap.org/survey2011/

PREFACE

In recent decades, the rapid development of information and communication technologies (ICTs) and their proliferation into all sectors of society have opened up new opportunities for socio-economic progress, poverty reduction and environmental sustainability. Yet, between and within countries, and among different areas, communities and socio-economic groups, there remains noticeable disparity in the access to ICTs and people's capacities to use them.

Bringing technologies to the people goes beyond the provision of infrastructure and hardware. The greatest need is for initiatives that encourage learning in different local contexts and exchanges of experiences and knowledge. As the World Summit on the Information Society outcome on Capacity Building states, "each person should have the opportunity to acquire the necessary skills and knowledge in order to understand, participate in, and benefit from the Information Society and Knowledge Economy." To this end, the Plan of Action calls for international and regional cooperation in the area of capacity building with an emphasis on creating a critical mass of skilled ICT professionals and experts.

In response to this call, the United Nations Asian and Pacific Training Centre for Information and Communication Technology for Development (UN-APCICT/ESCAP) was established on 16 June 2006 in Incheon, Republic of Korea as a regional institute of the United Nations Economic and Social Commission for Asia and the Pacific (UN/ESCAP). 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, Research and Knowledge Sharing, and Advisory Services. Together they form an integrated approach to ICT human capacity building.

A core activity based on the integrated approach is the *Academy of ICT Essentials for Government Leaders* (Academy), a flagship programme of APCICT. The Academy is a comprehensive ICT for development (ICTD) training curriculum 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. The Academy has reached thousands of individuals and hundreds of institutions throughout the Asia-Pacific and beyond since its official launch in 2008. The Academy has been rolled out in over 20 countries in the Asia-Pacific region, adopted in numerous government human resource training frameworks, and incorporated in the curricula of university and college programmes throughout the region. The Academy training curriculum with nine modules (and more forthcoming) has been translated into nine languages, and is available as an online course on the APCICT Virtual Academy in English, Bahasa Indonesia and Russian.

Complementing the Academy, APCICT has been conducting research on ICTD human resources development and promoting knowledge sharing among member countries on different aspects of ICTD through the development and dissemination of in-depth analyses, policy notes, case studies and best practices. APCICT also has an online knowledge sharing portal that includes: (1) a handful of communities of practice with a network of professionals committed to share knowledge and learn about different aspects of ICTD; and (2) the e-Collaborative Hub, a dedicated online platform used by about 900 members to enhance their learning and training experience through access to ICTD resources, training courses, news and events.

Based on a continuous demand for step-by-step “how-to” guidelines on different aspects of ICTD that translates technical details into a form that can be easily referenced, understood and applied by government officers, APCICT has created the Knowledge Sharing Series to further strengthen APCICT’s knowledge sharing efforts and strategically contribute to ICTD capacity building. The Knowledge Sharing Series is kindly supported by the Ministry of Strategy and Finance of the Republic of Korea, Korea Eximbank, and Korea Institute for Development Strategy.

The development of the Knowledge Sharing Series and this second issue in the series would not have been possible without the dedicated efforts of many individuals and organizations. I would like to specially acknowledge the authors of this second issue, Heung Youl Youm and Euisun Paik; and participants of the Second Asia-Pacific Regional Forum on ICT Human Capacity Development in October 2011 who attended and provided feedback on the session on “Cybersecurity as a National Priority”. I hope that this publication will offer useful insights and road maps that will help you better develop ICTD policies and research endeavours.

Hyeun-Suk Rhee
Director
UN-APCICT/ESCAP

ABOUT THE KNOWLEDGE SHARING SERIES

Growing demand for information and communications services, combined with technological innovation, growing infrastructure and falling prices, are allowing more and more people across the globe to participate in the information society.

The ICT revolution has resulted in many positive impacts, including raising the standard of living, increasing life expectancy, improving access to information, promoting lifelong learning, and connecting people to share, cooperate and innovate.

Despite these benefits, many policymakers and government officials have yet to acquire the knowledge and skills to leverage opportunities provided by ICTs and integrate ICT tools in the achievement of national development goals.

The Knowledge Sharing Series intends to help bridge the knowledge divide on how ICTs can be used for social and economic development, and ultimately help bridge the digital and development divide.

Aimed at policymakers and at government officials in operational departments and offices in developing countries, the series provide step-by-step guidelines, concrete strategies, proven best practices and select Case Studies on different aspects of ICT for development (ICTD). By making research findings, analyses and lessons learned easily accessible and comprehensible, the series can be useful for making informed decisions.

Each issue in the Series focuses on a specific ICTD theme, programme or project, and offers an end-to-end road map that can help policymakers in their planning, implementation, monitoring and evaluation processes.

This second issue of the Knowledge Sharing Series is focused on Cyberscurity. ICTs have created a borderless, always connected society with many social and economic benefits. But, this also means that there is a lot more information about us on the network that can fall in the hands of criminals. Critical infrastructure, information networks and communication systems are exposed to cyberattacks that can originate from anywhere in the world. The breakdown of these systems and networks can threaten national security and result in huge economic losses. Cybersecurity is about the protection of the physical networks and also the information that they hold. In a world where it is now predicted that there will be 50 billion connected devices by 2020, cybersecurity will continue to be at the top of most nation’s agenda in the years to come.

This second issue focuses on steps in developing cybersecurity policies and strategies, and in setting up and enforcing effective national cybersecurity initiatives to detect, prevent and mitigate cyberthreats.

TABLE OF CONTENTS

List of Figures

List of Tables

EXECUTIVE SUMMARY

As different types of cyberattacks are on the rise, cybersecurity threats are also growing rapidly. Most countries including developing countries in the Asia-Pacific region are at risk in cyberspace. And more than ever, cybersecurity vulnerabilities in government and critical information infrastructure are becoming sources of risks to national security, public safety and economic prosperity.

Since most critical infrastructures including electricity generation facilities, financial services, hospitals, transportation systems and water supply services are all increasingly dependent on information and communication technologies (ICTs) to function and deliver services efficiently, cyberattacks on these critical infrastructures may result in serious national security risks.

In addition, advanced persistent threats (APTs) are emerging risks that need to be responded to promptly by organizations as well as government agencies. APTs are made up of advanced malicious codes combined with sophisticated social engineering and a relentless target on government agencies and individual companies. APTs will have severe impacts on information assets of governmental organizations and businesses, especially since the target of APTs is often sensitive data and intellectual property. A governmental or private organization must recognize the requirements to adopt defensive mechanisms through governance, risk management and control to ensure that threats are acted upon immediately.

Cybersecurity has moved to the top of the international agenda recently, as high profile attacks on public and private organizations have become more frequent. Cyberthreats of all types combine to present organizations with a new risk profile that must be evaluated alongside more traditional business risks. In addition to potential economic loss and brand damage as a result of criminal cyberattacks and cyberactivism activities, organizations also need to take into account other types of related cyber-risks such as intellectual property theft, physical damage to information assets and business disruption. Despite all the advantages that are attributed to today's Internet-connected world, there is no doubt that, from a risk perspective, it comes at a potential cost.

Therefore, a deep understanding of cybersecurity threats and the countermeasures for these attacks is necessary for policymakers in order to build a foundation of knowledge to secure next generation networks. Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment, the organization and users' assets. In short, cybersecurity encompasses all the necessary elements required to defend and respond to cyberthreats in cyberspace.

Cyberseurity has been recognized as one of the important tools that can support the provision of secure ICT services. Thus, it is critical to design proper arrangements for steering and coordinating the whole process of policy planning, implementation, monitoring and evaluation among various levels of government authorities and agencies. Experiences learned from many countries show a considerable degree of failure in coordinating cybersecurity effectively.

According to a recent needs assessment survey conducted by UN-APCICT/ESCAP that engaged policymakers from 29 countries, the development of cybersecurity strategies is viewed by policymakers as one of the impending tasks that needs to be addressed to increase the success rate of national cybersecurity initiatives.

Steps for developing cybersecurity policies and strategies include the following:

- Persuading national government leaders at the highest level
- Identifying a lead person and institution for the overall national effort
- Identifying the appropriate experts and policymakers
- Identifying cooperative arrangements for and among all participants
- Establishing mechanisms for cooperation among government and private sector entities at the national level
- Identifying international counterparts and fostering international efforts to address cybersecurity issues
- Establishing an integrated risk management process for identifying and prioritizing protective efforts regarding cybersecurity
- Assessing and periodically reassessing the current state of cybersecurity efforts and developing programme priorities
- Identifying training requirements and how to achieve them

This second issue of the Knowledge Sharing Series on cybersecurity is complemented by Module 6 of the *Academy of ICT Essentials for Government Leaders* (*Academy*) on information security and privacy. The *Academy* is a comprehensive ICT for development training curriculum for policymakers and government leaders developed by UN-APCICT/ESCAP.

Module 6 of the *Academy* provides the fundamental knowledge on information security and privacy. It clarifies the concept of information security, privacy and related concepts, including threats to information security and how they can be addressed. The module discusses the requirements for the establishment and implementation of policy on information security, as well as the life cycle of information security policy; and provides an overview of standards for information security and privacy protection that are used by some countries and international information security organizations.

This publication identifies the reasons why developing countries need to develop a comprehensive national cybersecurity policy and strategies. More importantly, it provides a step-by-step guide to help policymakers set up cybersecurity policies and strategies, and implement cybersecurity programmes in their countries. Case Studies with best practices and lessons learned from selected countries will be shared.

The publication addresses critical, indispensable components of cybersecurity such as critical information infrastructure protection (CIIP), public key infrastructure (PKI), national incident management, common criteria for ICT products, information security management, personal information protection, cybercrime law and e-government security. The publication also provides materials that address various aspects required for the establishment, implementation, evaluation and improvement of national cybersecurity strategies and programmes that are being implemented in the developing countries of the Asia-Pacific region.

The contents of this publication are organized as follows:

- Chapter 1 gives an overview of the threats in cyberspace and defines cybersecurity. It also examines the relationship between cybersecurity and other security domains.

- Chapter 2 is on cybersecurity strategies and discusses the reasons for establishing a national cybersecurity strategy and the steps for establishing the national cybersecurity strategy. These steps include: (1) persuading national government leaders; (2) identifying a lead person and institution for the overall national effort; (3) identifying suitable experts and policymakers; (4) establishing cooperative arrangements and mechanisms; (5) collaborating with international counterparts; (6) developing an integrated risk management process for identifying and prioritizing protective efforts; (7) assessing and periodically reassessing the state of cybersecurity efforts; and (8) identifying and meeting training needs. Case Studies from Australia, Japan, the Republic of Korea and the UK are presented.

- Chapter 3 is on CIIP and looks at: (1) the concept of CIIP; (2) CIIP vulnerabilities—unauthorized access to sensitive or confidential information, destruction, modification or substitution of software needed by critical infrastructures, and limited access for the agents able to prevent or mitigate the results of the attacks; (3) CIIP objectives—preventing cyberattacks on critical infrastructures, reducing national vulnerabilities to cyberattacks, and minimizing damage and recovery time from cyberattacks that do occur; (4) the four tasks for CIIP—prevention and early warning, detection, reaction, and crisis management; and (5) countermeasures that can be taken at the national level and international levels for CIIP. CIIP Case Studies from Australia, Japan, the Republic of Korea and the United States of America are presented.

- Chapter 4 is on the PKI and explains the concept of public key algorithms in which a public key can be made widely public but the private key must always be kept confidential. The sender encrypts the message with the recipient's public key, and the recipient decrypts it with their corresponding private key. The chapter looks at: (1) the components of the PKI—an end-entity, a certification authority, a registration authority and a repository; and (2) steps for establishing a national PKI—establishing the digital signature act, determining the organizational structure for a national PKI, developing the certification policy and certification practice statement that can be used by the certification authorities, and performing a periodic or on-demand audit for the certification authority to check if they comply with the legal requirements of the digital signature act. PKI Case Studies from the Republic of Korea and Luxembourg are presented.

- Chapter 5 is on national incident management and gives: (1) an overview of incident management for organizations; and (2) the reasons and steps for establishing a national Computer Emergency Readiness Team (CERT). The steps include establishing a legal framework, setting up an institution responsible for coordinating and overseeing a national CERT, and establishing a plan for CERT operation, international collaboration and funding. Case Studies on the legal framework, policies and strategies for national incident management in Finland and the Republic of Korea are presented.

- Chapter 6 is on the Common Criteria (CC) for information security solutions and provides: (1) an overview of the CC as an international standard (ISO/IEC 15408) and the Common Criteria Recognition Arrangement; (2) a structure of the CC for information security solutions' evaluation; and (3) four evaluation and assessment procedures for acquiring CC certification. They are preparation, evaluation, certification and follow-up.

- Chapter 7 is on personal information protection and examines: (1) the legal concept and history of personal information protection; (2) specified measures for personal information protection—legal and regulatory measures, technical measures and cultural measures; and (3) the legal and regulatory trends of member countries of the Organisation for Economic Co-operation and Development (OECD). As the proper handling of personal information by public and private sectors become critical, the legal basis to protect citizen's personal information needs to be prepared and enforced. Furthermore, it is important to establish an independent personal information protection supervisory authority in order to carry out overall duties for protection of citizens' privacy and rights. The OECD has developed a number of guidelines on personal information protection. The OECD's eight principles for personal information protection are the minimum standards that are recommended to its member countries, and they have been widely used in the enactment of personal information protection laws.

- Chapter 8 is on cybercrime law and legislation. It offers the definition and classification of cybercrime, and the steps required to establish cybercrime laws and legislations. The steps include: (1) assessing the current legal authorities for adequacy; (2) drafting and adopting substantive, procedural and mutual assistance laws and policies to address cybercrime;

(3) establishing or identifying national cybercrime units; (4) developing cooperative relationships with other elements of the national cybersecurity infrastructure and the private sector; (5) developing an understanding among prosecutors, judges and legislators of cybercrime issues; and (6) participating in the 24/7 Cybercrime Point of Contact Network. Case Studies of cybersecurity-related laws in the European Union and the Republic of Korea are presented.

- Chapter 9 is on the information security management system (ISMS) and discusses: (1) the ISMS management process; (2) requirements for ISMS documentation; and (3) the information security control structure. The ISMS consists of processes and systems to ensure confidentiality, integrity and availability of information assets while minimizing security risks. Most accredited certification bodies are certifying the ISMS according to ISO/IEC 27001. The certification process of ISMS consists of three stages. The first stage is to familiarize the evaluators with the organization. The second stage is to test the ISMS requirements specified in ISO/IEC 27001. The third stage includes follow-up activities after certification. Applicants of ISMS certification need to establish and implement managing processes, documentation requirements and control structure.

- Chapter 10, the final chapter of the publication, wraps up with a look at the concept of a culture of cybersecurity, which refers to the necessity of all participants to review their approach to ICTs and make adjustments to help ensure cybersecurity. Nations are encouraged to develop throughout their societies a culture of cybersecurity in the application and use of ICTs. At the same time, a global culture of cybersecurity is also required as cybersecurity issues transcend national boundaries. Steps toward creating a culture of cybersecurity are as follows:

    - Develop and implement a cybersecurity plan for government-operated systems
    - Implement security awareness programmes and initiatives for users of systems and networks
    - Encourage the development of a culture of security in business enterprises
    - Support outreach to civil society with special attention given to the needs of children and youth, persons with disabilities, and individual users
    - Promote a comprehensive national awareness programme so that all participants—businesses, the general workforce and the general population—secure their own portions of cyberspace
    - Enhance science and technology, and research and development (R&D) activities
    - Review existing privacy regime and update it to the online environment
    - Develop awareness of cyber-risks and available solutions

This publication is targeted at (but is not limited to):

- Policymakers at the national and local government levels in developing countries who are responsible for cybersecurity policymaking;
- Government officials of developing countries who are responsible for the development and implementation of cybersecurity-based applications; and
- Managers in the public or private sector in developing countries seeking to employ cybersecurity tools for project management.

This publication represents the beginning of the journey to understanding, exploring and sharing knowledge on the different aspects of cybersecurity. UN-APCICT/ESCAP has created an ICT for development community of practice, that is “an interactive network of committed professionals bound by a common interest in ICT for development.” It has an online workspace for its members that will serve as an effective platform for mutual learning and sharing of knowledge and experiences on cybersecurity.

Acronyms

APCICT	Asian and Pacific Training Centre for Information and Communication Technology for Development (United Nations)
APT	Advanced Persistent Threat
BCA	Bridge Certification Authority
CA	Certification Authority
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CERT	Computer Emergency Readiness Team or Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CSIRT	Computer Security Incident Response Team
CTL	Certificate Trust List (Republic of Korea)
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service
EAL	Evaluation Assurance Level
ESCAP	Economic and Social Commission for Asia and the Pacific (United Nations)
EU	European Union
FCD	Final Committee Draft
FICORA	Finnish Communications Regulatory Authority
G8	Group of Eight
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISPC	Information Security Policy Council (Japan)
IT	Information Technology
ITSEAG	Information Technology Security Expert Advisory Group (Australia)
ITU	International Telecommunication Union
KCC	Korea Communications Commission
KISA	Korea Internet and Security Agency
KrCERT	Korea Computer Emergency Response Team
KrCERT/CC	Korea Computer Emergency Response Team Coordination Center
MIC	Ministry of Information and Communication (Republic of Korea)
MOPAS	Ministry of Public Administration and Security (Republic of Korea)
NCSC	National Cyber Security Center (Republic of Korea)
NISC	National Information Security Center (Japan)
OECD	Organisation for Economic Co-operation and Development
PKI	Public Key Infrastructure
POC	Point-of-Contact
R&D	Research and Development
TISN	Trusted Information Sharing Network (Australia)
TOE	Target of Evaluation
UK	United Kingdom
US	United States
USA	United States of America

1. AN INTRODUCTION TO CYBERSECURITY

You will find in this chapter discussions on:

- **The concept of cyberspace, cyberthreats and cybersecurity; and**
- **The relationship between cybersecurity and other security domains.**

1.1 Cyberspace and Cyberthreats

Network connectivity and remote access is critical to cyberspace. However, widespread access to and the loose coupling of interconnected information and communication technology (ICT) systems can be a primary source of widespread vulnerabilities. In cyberspace, vulnerabilities are becoming the target of cybersecurity threats. These threats include viruses, worms, Trojan horses, malware, spyware, adware, spoofing attacks, identity theft, spam and cyberattacks, all of which are on the rise. In this chapter, the concepts of cyberspace and cybersecurity are defined in order to build the foundation for securing the networks of tomorrow and today.

Cyberspace represents the new medium of communication—electronic communication. It can be described as a virtual environment, the electronic medium of computer networks, in which online communication takes place. Cyberspace is a complex environment or space resulting from the emergence of the Internet. The networked environment is made up of people, organizations, activities, services and technology devices. Cybersecurity is about the security of this complex virtual environment or virtual world.

In online gaming, for example, many virtual worlds may have a virtual currency that is used to buy in-game items on the Internet game sites. Consequently, there is an associated real world value to the virtual currency and even in-game items. These virtual items are frequently traded for real currency on online auction or game sites and some games even have an official channel with published virtual/real currency exchange rates for the monetization of virtual items. It is these monetization channels that make these virtual worlds a target for attack, usually by phishing or other techniques for stealing account information.

Cyberthreats can be classified as accidental or intentional and may be active or passive. Accidental threats are those that exist with no premeditated intent. Examples of realized accidental threats include system malfunctions, operational blunders and software bugs. Intentional threats may range from casual examination, using easily available monitoring tools, to sophisticated attacks using special system knowledge. An intentional threat, if realized, may be considered to be an “attack”. Passive threats are those that, if realized, would not result in any modification to any information contained in the system(s), and where neither the operation nor the state of the system is changed. The use of passive wire tapping to observe information being transmitted over a communications line is a realization of a passive threat. Active threats to a system involve the alteration of information contained in the system, or changes to the state or operation of the system.

Threats affect assets, so the first step is to list out the assets that require protection. The next step of the assessment is a threat analysis, then a vulnerability analysis (including impact assessment). Based on the results of these assessments, countermeasures and security mechanisms are put in place. The basic steps in cybersecurity are as follows:

- Identify the vulnerabilities of the system;
- Analyse the likelihood of threats aimed at exploiting these vulnerabilities;
- Assess the consequences if each threat were to be successfully carried out;
- Estimate the cost of each attack;
- Cost out potential countermeasures; and
- Select the security mechanisms that are justified (possibly by using a cost/benefit analysis).

In some cases, non-technical measures, such as insurance coverage, may be a cost effective alternative to technical security measures. In general, perfect technical security is not possible. The objective, therefore, should be to make the cost of an attack high enough to reduce the risk to acceptable levels.

1.2 Cybersecurity

Organizations or countries should set up a comprehensive plan for mitigating its security threats and meeting security requirements to protect their cyberspace. That means that organizations are encouraged to view cybersecurity as an indispensable process to protect systems, networks, applications, services and resources.

The term cybersecurity can be regarded as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment and organization and users' assets according to the International Telecommunication Union (ITU) Recommendation X.1205.[1] The organization and users' information and ICT assets may include interconnected computing devices, mobile devices, personnel, infrastructure, applications, services, telecommunications systems, and all the transmitted and/or stored information in the cyberenvironment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and users' information assets against relevant security risks in the cyberenvironment. The general security objectives comprise the following:

- Availability
- Integrity, which may include message or entity authenticity and non-repudiation
- Confidentiality

Cybersecurity techniques can be used to ensure system availability, integrity, authenticity, non-repudiation and confidentiality. In addition, cybersecurity can be used to ensure that users' privacy be respected. Cybersecurity techniques can be used to increase the users' trust in the information and assets of the organization.

The cyberenvironment includes the software that runs on computing devices, and the stored (also transmitted) information on these devices or information that are generated by these devices. Installations and buildings that house the devices are also part of the cyberenvironment. Cybersecurity needs to take all these elements into consideration.

Cybersecurity aims at securing the cyberenvironment, a system that may involve a number of stakeholders that belong to many public and private organizations, using diverse components and different approaches to security. As such, it is beneficial to think of cybersecurity in the following senses:

- The collection of policies and actions that are used to protect connected networks (including computers, devices, hardware, stored information and information in transit) from unauthorized access, modification, theft, disruption, interruption or other threats.
- An ongoing evaluation and monitoring of the above policies and actions in order to ensure the continued quality of security in the face of the changing nature of threats.

1 ITU, Recommendation ITU-T X.1205, Overview of cybersecurity, April 2008.

1.3 The Relationship between Cybersecurity and Other Domains[2]

Cybersecurity is not a synonym for Internet security, network security, application security, information security or critical information infrastructure protection (CIIP). It has a unique scope requiring stakeholders to play an active and preventive role in order to maintain, if not improve the usefulness and trustworthiness of cyberspace. There are differences between cybersecurity and other domains of security as follows:

- Information security is concerned with the protection of confidentiality, privacy, integrity and availability of information in general, to serve the needs of the applicable information user.

- Application security is a process performed to apply controls and measurements to an organization's applications in order to manage the risk of using them. Controls and measurements may be applied to the application itself (its processes, components, software and results), to its data (configuration data, user data, organization data), and to all technology, processes and actors involved in the application's life cycle.

- Network security is concerned with the design, implementation and operation of networks for achieving the purposes of information security on networks within organizations, between organizations, and between organizations and users.

- Internet security is concerned with protecting Internet-related services and related ICT systems and networks as an extension of network security in organizations and at home, to achieve the purpose of security. Internet security also ensures the availability and reliability of Internet services.

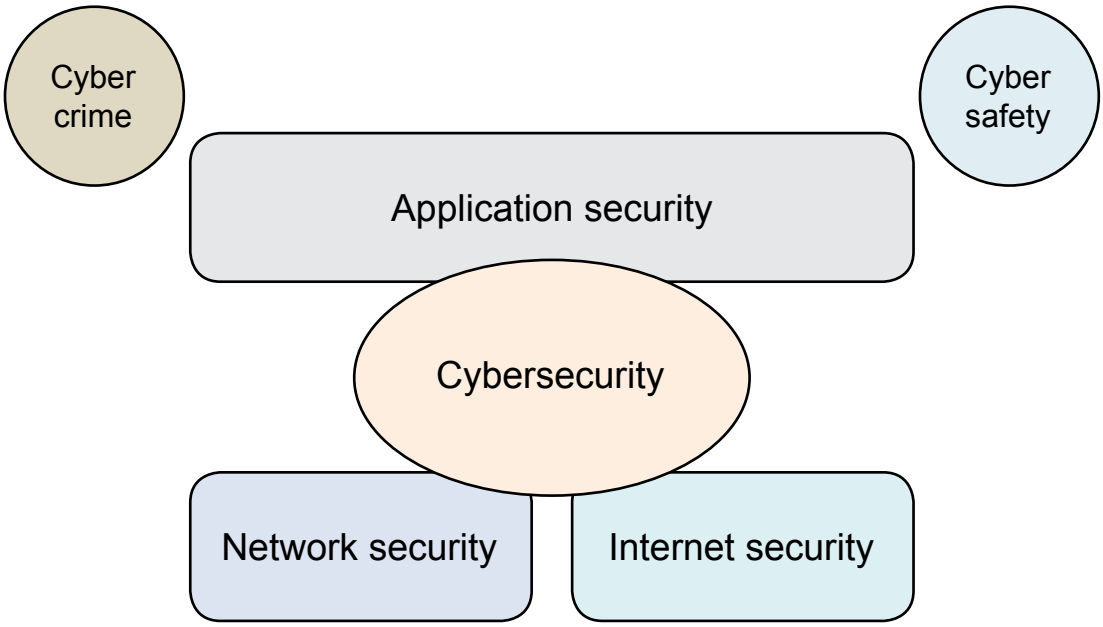
- CIIP is concerned with protecting the systems that are provided or operated by critical infrastructure providers, such as energy, telecommunications and water departments. CIIP ensures that those systems and networks are protected and resilient against information security risks, network security risks, Internet security risks, as well as cybersecurity risks.

Figure 1 describes the relationship between cybersecurity and other domains of security. The relationship between these security domains and cybersecurity may be complex. Some of the critical infrastructure services, for example water and transportation, need not impact the state of cybersecurity directly or significantly. However, the lack of cybersecurity can have a negative impact on the availability of critical information infrastructure systems provided by the critical infrastructure providers.

On the other hand, the availability and reliability of the cyberspace in many ways relies on those related critical infrastructure services, such as the telecommunications network infrastructure. The security of the cyberspace is also closely related to the security of the Internet, enterprise/home networks and information security in general. It should be noted that the security domains identified in this section have their own objectives and scope of focus. Dealing with cybersecurity issues, therefore, requires substantial communication and coordination between different public and private entities from different countries and organizations. Critical infrastructure services are regarded by some governments as critical services related to national security, and therefore may not be discussed openly. Furthermore, knowledge of critical infrastructure weaknesses, if not used appropriately, can have direct implications for national security. A basic framework for information sharing and issue or incident coordination is therefore necessary to bridge the gaps and provide adequate assurance to the stakeholders in cyberspace.

2 This chapter draws on ITU, Recommendation ITU-T X.1205, Overview of cybersecurity, April 2008; and on ISO/IEC FCD 27032, Information technology—Security techniques—Guidelines for cybersecurity, May, 2011.

Figure 1. The relationship between cybersecurity and other security domains



Source: Adapted from ISO, ISO/IEC FCD 27032, Information technology—Security techniques—Guidelines for cybersecurity, May, 2011.

2. NATIONAL CYBERSECURITY STRATEGIES

You will find in this chapter discussions on:

- **The concept of cybersecurity strategy;**
- **Why a national cybersecurity strategy is needed;**
- **How to establish a national cybersecurity strategy; and**
- **Case Studies on the national cybersecurity strategies of Australia, Japan, the Republic of Korea and the United Kingdom (UK).**

2.1 Overview

Every day, millions of people across the world rely on the ICT services and information in cyberspace: that is, all forms of networked, digital activities. They may be aware of this if surfing the Web, shopping online or social networking, or they may be unaware of the networked activity underpinning the ICT services they rely on, and of just how critically dependent the works of government, business and national infrastructure are on this relatively new domain of human activity. Either way, the effective functioning of cyberspace is of vital importance to the works of people, business and government, and cyberthreats can have huge impacts on their functioning.

Beginning on 4 July 2009, a series of distributed denial-of-service (DDoS) attacks were launched, first on Korean websites, and then on both Korean and United States (US) government and commercial websites.[3] The websites targeted included the Korean Assembly, the American and Korean Presidents' websites, the US State Department, major public websites for the US stock exchanges—NYSE and NASDAQ—and popular portal websites in the Republic of Korea such as "naver.com". Investigations revealed that the attack was done using a botnet that was apparently built using a variant of the MyDoom worm from early 2004 together with rudimentary DDoS attacks such as the HyperText Transfer Protocol request floods, and the User Datagram Protocol and Internet Control Message Protocol floods. The attacks continued until 10 July, and the infected computers were programmed to encrypt files and render themselves unbootable.

These DDoS attacks that took place in the Republic of Korea and the United States of America (USA) in 2009,[4] and the Republic of Korea in 2011[5] alerted countries to the fact that: (1) most countries are at risk to cyberattacks; (2) the threats to information security could be threats to national security; and (3) effective, immediate crisis management from those cyberattacks are urgently required.

2.2 Steps for Establishing a Cybersecurity Strategy

Information security risks are becoming more diversified, advanced, organized and complex, and many conventional means of security fail to ensure information security. That is why a new, comprehensive national cybersecurity strategy is needed. In order to accurately respond to such challenges in the information security environment, many countries have established their cybersecurity strategies to reinforce the defence capability against cyberattacks. A national cybersecurity strategy should recognize the challenges of cybersecurity and the need for addressing them. It should also stress a need for a coherent, consistent, coordinated and systematic approach to cybersecurity in which the government, organizations across the public and private sectors, and international partners all work together. In addition, the national cybersecurity strategy should include organized and prompt countermeasures to ensure national security and effective crisis management against cyberattacks.

For example, the Japanese government developed new information security initiatives in response to the major changes in the information security environment, and at the same time, continued to manage the implementation of the Second National Strategy on Information Security being undertaken by governmental/private entities in 2009.[6] The Korean government also drew

3 Steven Adair, "Korean/U.S. DDoS Attacks - Perplexing, Disruptive, and Destructive", 10 July 2009. Available at http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20090710 (accessed on 10 January 2012).

4 Jason Mick, "Massive DDOS Attacks on U.S., South Korea, Came From the UK, Researcher Says", *DailyTech*, 15 July 2009. Available at http://www.dailytech.com/Massive+DDOS+Attacks+on+US+South+Korea+Came+From+the+UK+Researcher+Says/article15690.htm (accessed 10 January 2012).

5 Koo Bon-kwon, "Massive DDoS attack returns to S.Korea", *Hankyoreh*, 5 March 2011. Available at http://english.hani.co.kr/arti/english_edition/e_national/466626.html (accessed on 10 January 2012).

6 Information Security Policy Council, Information Security Strategy for Protecting the Nation, Japan, 11 May 2010. Available at http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf (accessed on 10 January 2012).

up the Master Plan on National Cybersecurity.[7] In 2009, Australia launched a cybersecurity strategy to formalize the roles, responsibilities and policies of Australian intelligence, cyber and policing agencies to protect Australian Internet users.

The national cybersecurity strategy may consist of a number of mutually reinforcing initiatives with the following major goals designed to help secure the country in cyberspace:

- To establish a modernized, flexible defence strategy against today's immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats and events within the government—and ultimately with state and local governments and private sector partners—and the ability to act quickly to reduce current, imminent vulnerabilities and prevent incidents.

- To defend against the full range of security threats by enhancing response capabilities and increasing the security of the supply chain for key information technologies.

- To strengthen the future cybersecurity capability by expanding cybereducation; coordinating and redirecting R&D efforts across the government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.

The foregoing goals are common to all countries; however, the specific steps taken to implement these goals will vary according to each country's unique status, needs and circumstances. In many countries, the national government should undertake some steps. Here are the key steps for establishing cybersecurity strategy, as recommended by ITU.[8]

- **Persuade national government leaders at the highest level of the need for national action** to address threats to and vulnerabilities of the national cyberinfrastructure through policy-level discussions

    - For a nation seeking to enhance cybersecurity and secure its critical information infrastructure, a first step is to establish cybersecurity as national policy. In general, a national cybersecurity policy statement: (1) recognizes the importance of the critical information infrastructure to the nation; (2) identifies the risks it faces; (3) establishes the cybersecurity policy goal; and (4) broadly identifies how it will be implemented, including through collaboration with relevant stakeholders. Once an overall cybersecurity policy is clearly defined, it can be amplified by a national strategy that delineates roles and responsibilities, identifies priorities, and establishes time frames and metrics for implementation. Additionally, the policy and strategy may also place the national efforts in the context of other international cybersecurity activities. In order to achieve an overall cybersecurity policy, it may be necessary to raise awareness of the issues among key decision makers. The decision makers need to understand that it may take a long period to achieve the agreed upon cybersecurity goals.

    - A national cybersecurity framework should be flexible and able to respond to the dynamic risk environment. The framework should establish policy goals. By establishing clear policy goals, government agencies and non-government entities can work together to achieve the stated goals in the most efficient and effective manner.

7 Xinhua, "S.Korea draws up master plan on national cyber security", 8 August 2011. Available at http://news.xinhuanet.com/english2010/world/2011-08/08/c_131036656.htm (accessed on 10 January 2012).

8 These steps are drawn heavily from: ITU, "ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts", draft, January 2008. Available at http://www.itu.int/ITUD/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf (accessed on 10 February 2010).

- This national policy should be developed cooperatively through consultation with representatives of all relevant participant groups including government agencies, the private sector, academia, industries and relevant associations. This policy should be promulgated at the national level, preferably by the top-level of government.

- **Identify a lead person and institution for the overall national effort**

  - The Computer Security Incident Response Teams (CSIRTs) with national responsibility provides the necessary services to handle information security related issues and assist their constituents to recover from breaches. CSIRTs are also sometimes called Computer Emergency Response Teams or Computer Emergency Readiness Teams (CERTs). While CSIRTs and CERTs perform the same function, the term "computer" in CSIRT is used inclusively in this publication to encompass routers, servers, IP-mobile devices and related applications.[9]

  - The launch of a cybersecurity initiative requires the identification of a lead person in the initial phase to steer the national cybersecurity effort. This is usually a person in government at the policy level who understands the issues of cybersecurity, can direct and coordinate the efforts of governmental institutions, and can effectively interact with the private sector. Ideally this person should have political stature and access to the head of government. This high-level authority is necessary to ensure the coordination among entities that need to interact. In time, this coordination effort will provide an institutional foundation on which the country's cybersecurity technical leaders and organizations can build upon.

- **Identify the appropriate experts and policymakers** within government authorities and private sector, and their roles in developing and implementing different parts of the national cybersecurity strategy

  - Effective national action requires the inculcation of a "culture of cybersecurity" among all participants. All individuals and institutions within government and outside of government that develop, own, provide, manage, service, and use information systems and networks must understand the role they need to play and the actions that need to be taken. Senior policymakers and leaders of the private sector must establish goals and priorities within their institutions. Senior technical experts must provide guidelines and frameworks for action.

- **Identify cooperative arrangements for and among all participants**

  - National government should foster both formal and informal collaborative arrangements that permit and encourage communication and information sharing between government and the private sector. Cybersecurity will be implemented at the technical or operational level by a wide array of institutions, both governmental and non-governmental. These efforts must also be coordinated and include mechanisms for information sharing.

- **Establish mechanisms for cooperation among government and private sector entities at the national level**

  - Policy development and the elaboration and implementation of the national plan must be undertaken through open and transparent processes. These efforts must take into account the views and interest of all participants.

9 http://www.enisa.europa.eu/act/cert is a good website for more information on CERTs and CSIRTs.

- **Identify international counterparts and foster international efforts to address cybersecurity issues**, including information sharing and assistance efforts

    - The effort to improve national cybersecurity will be helped by participating in regional or international forums, including conferences and workshops, which can provide education and training. Such forums raise awareness of the issues, provide expert presentations and offer the opportunity for countries to share their ideas, experiences and perspectives. Participation and/or membership in regional as well as international organizations working toward similar goals can also assist in this effort to improve national cybersecurity.

    - Participation in available programmes and activities of multilateral organizations that seek to improve and enhance global cybersecurity is another way to foster international collaboration.

    - In addition, participation in efforts led by the private sector, such as the Anti-Phishing Working Group and other similar international endeavours, should also be considered.

- **Establish an integrated risk management process for identifying and prioritizing protective efforts regarding cybersecurity**.

    - Only by understanding risks can government and infrastructure owners and operators (including the vendors who support them) begin a public-private-peoples' collaboration to identify and prioritize key functions and elements for protection. Once identified, the critical information infrastructure functions can be prioritized or ranked as to which is most important and in what context. It is important to remember that the notion of "criticality" is situation-dependent, and what could be critical in one instance may not be critical in the next. As nations identify and prioritize critical functions, they need to remember that criticality will change with technology, infrastructure and process enhancements.

    - Protecting critical information infrastructure and cyberspace and the critical functions comprised therein is very challenging and involves the continuous application of a series of risk management practices. They include: assessing threat, vulnerability and consequence; (2) identifying controls and mitigations; (3) implementing controls; and (4) measuring effectiveness. Together these practices enable operators to manage risks and ensure resilience across their essential missions. Individually, information infrastructure providers generally have sophisticated risk management methodologies and practices in place because of the real-time nature of the services they deliver. However, the interconnectivity, interdependence and technical complexity of the information infrastructure limit the ability to easily assess overall risk or readiness. As a result, there is a significant benefit to leveraging public-private collaborations to assess the shared dependencies and infrastructure risks (natural disaster, technological failure, terrorist attack, etc.)

- **Assess and periodically reassess the current state of cybersecurity efforts and develop programme priorities**

    - The national cybersecurity strategy should include a national assessment survey, which could be used for self-evaluation of progress being made or as part of training or a supported assessment effort. By utilizing a common self-assessment tool, countries can identify strengths and potential gaps in their national framework and establish a process for aligning them with their desired goals.

- **Identify training requirements and how to achieve them**

  - By conducting a gap analysis, a country may find that there are aspects of its cybersecurity programme that need improvement. The solutions may be technical (e.g., new equipment or software), legal (e.g., drafting new laws or regulations to address inappropriate cyberconduct), or organizational. A gap analysis is also likely to reveal where additional human capacity building (including training) is needed.

2.3 Case Studies

2.3.1 Republic of Korea

Since the major cyberattack that halted Internet services in the Republic of Korea on 25 January 2003, the Korean government has established and implemented intermediate cybersecurity plan regularly. In August 2011, the Korea Communications Commission (KCC)[10] announced the cybersecurity master plan prepared in collaboration with all 15 relevant ministries, including the National Information Service, the Ministry of Public Administration and Security (MOPAS), and the Prime Minister's Office. The master plan aimed to improve the cybersecurity preparedness and capability to protect national assets from massive, organized cyberattacks, such as a 7.7 massive DDoS attack[11] and a 3.4 DDoS attack.[12]

The aim of a national cybersecurity master plan is to prevent, detect, respond to and recover from cyberterrorist attacks. According to the KCC, cyberspace in the master plan is considered as another operational domain similar to the nation's territories on land, air and sea that need a state-level defence system.

Under the master plan, the National Cyber Security Center (NCSC),[13] run by the National Intelligence Service,[14] the country's information agency, will serve as a control tower to coordinate efforts against cyberattacks among government agencies involving the KCC, and the ministries of defence and home affairs.

The master plan requires government agencies and private enterprises to encrypt and back up important data, and install necessary licensed software to prevent hackers' attacks. According to the KCC, each government agencies involved in the master plan are deliberating detailed action plans for their respective duties.

2.3.2 Australia[15]

Australia launched its Cybersecurity Strategy in 2009 to formalize the roles, responsibilities and policies of Australian intelligence, cyber and policing agencies to protect Australian Internet users. The overall aim of Australia's cybersecurity policy is: "the maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security

10 http://eng.kcc.go.kr/user/ehpMain.do.

11 Jane Han, "Fresh Cyber Attacks Expected Thursday Evening", *The Korea Times*, 8 July 2009. Available at http://www.koreatimes.co.kr/www/news/biz/2009/07/123_48138.html (accessed on 6 January 2011).

12 "Web sites hit by new DDoS attack", *The Korea Times*, 5 March 2011. Available at http://www.koreatimes.co.kr/www/news/nation/2011/03/113_82520.html (accessed on 6 January 2011).

13 http://service1.nis.go.kr.

14 http://eng.nis.go.kr/svc/index.do.

15 This section is drawn heavily from: CERT Australia, "About Us". Available at http://www.cert.gov.au/www/cert/cert.nsf/Page/About_Us (accessed on 14 February 2012).

and maximizes the benefits of the digital economy."[16] The Cybersecurity Strategy articulates the overall aim and objectives of the Australian government's cybersecurity policy and sets out the strategic priorities that the Australian government will pursue to achieve these objectives.

The strategy brought together Australia's existing computer emergency response arrangements under a new national CERT, CERT Australia,[17] which commenced operation in January 2010. The strategy details CERT Australia's roles and responsibilities, which is to work with the private sector in identifying critical infrastructure and systems that are important to Australia's national interest, based on an assessment of risk, and to provide these organizations with information and assistance to help them protect their ICT infrastructure from cyberthreats and vulnerabilities. CERT Australia is also a source of cybersecurity information for the Australian community and the point of contact for Australia's international cybersecurity counterparts. It also has a coordination role in the event of a serious cyberincident.

The strategy also provides the roles and responsibilities of the Cyber Security Operations Centre, which was established as an initiative of the Australian Government's Defence White Paper. It serves the Australian government by providing a comprehensive situational awareness of the cyberthreat and the security status of government networks. It is also responsible for facilitating operational responses to cybersecurity events of national importance.

CERT Australia and the Cyber Security Operations Centre have complementary roles in ensuring that Australia is protected from cyberthreats. CERT Australia contributes to the Cyber Security Operations Centre's ability to form a national picture of cyberthreats for the Australian government. The Cyber Security Operations Centre provides information to CERT Australia that can be used to help protect the Australian community.

2.3.3 Japan

In May 2010, the Information Security Policy Council of Japan published its Information Security Strategy for Protecting the Nation.[18] It defines three basic policies: (1) reinforcement of policies taking account of possible outbreaks of cyberattacks and establishment of a counteractive organization; (2) establishment of policies adapted to changes in the information security environment; and (3) by 2020, Japan aims to become the world's foremost "advanced information security country" through establishing an environment where the entire nation can use ICT safely (an environment where high quality, reliability, safety and security are ensured).

2.3.4 United Kingdom

The Cyber Security Strategy of the UK[19] provides a coherent approach that aims at reducing risk from the UK's use of cyberspace, exploiting opportunities in cyberspace and improving knowledge, capabilities and decision-making. The strategy recognizes the role of public and private sectors, international partners, and GovCertUK, the CERT for the UK government.[20] It also provides for the establishment of structures such as the Office of Cyber Security to ensure strategic leadership for and coherence across government; and a Cyber Security Operations Centre to actively monitor the health of cyberspace and coordinate incident response, enable better understanding of attacks against UK networks and users, and provide better advice and information about the risks to business and the public.

16 Australian Government, *Cyber Security Strategy* (2009). Available at: http://www.ag.gov.au/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf (accessed on 10 January 2012).

17 http://www.cert.gov.au.

18 Information Security Policy Council, Information Security Strategy for Protecting the Nation, Japan, 11 May 2010. Available at http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf (accessed on 10 January 2012).

19 Cabinet Office, *Cyber Security Strategy of the United Kingdom* (Norwich, The Stationery Office, 2009). Available at: http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf (accessed on 10 January 2012).

20 http://www.govcertuk.gov.uk.

Summary

- Why develop a national cybersecurity strategy?
  - To take organized and prompt countermeasures to ensure national security and effective crisis management against cyberattacks by recognizing the challenges of cybersecurity and the need for addressing them
  - To stress the needs for a coherent, consistent, coordinated and systematic approach to cybersecurity
  - To put in place the organizational structures for cybersecurity and outline the roles and responsibilities for the different organizations working in the area of cybersecurity
- What are the ITU recommendations for establishing national cybersecurity strategies?
  - Persuading national government leaders at the highest level
  - Identifying a lead person and institution for the overall national effort
  - Identifying the appropriate experts and policymakers
  - Identifying cooperative arrangements for and among all participants
  - Establishing mechanisms for cooperation among government and private sector entities at the national level
  - Identifying international counterparts and fostering international efforts to address cybersecurity issues
  - Establishing an integrated risk management process for identifying and prioritizing protective efforts regarding cybersecurity
  - Assessing and periodically reassessing the current state of cybersecurity efforts and develop programme priorities
  - Identifying training requirements and how to achieve them

This chapter can be used when policymakers establish a national cybersecurity strategy for their countries.

3. CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

You will find in this chapter discussions on:

- **An overview of the CIIP;**
- **The CIIP objectives, major tasks for CIIP, and CIIP measures at the national level and international level; and**
- **Case Studies on the CIIP and the institutional arrangements for CIIP in Australia, Japan, the Republic of Korea and the USA.**

3.1 Overview

3.1.1 Critical Infrastructure

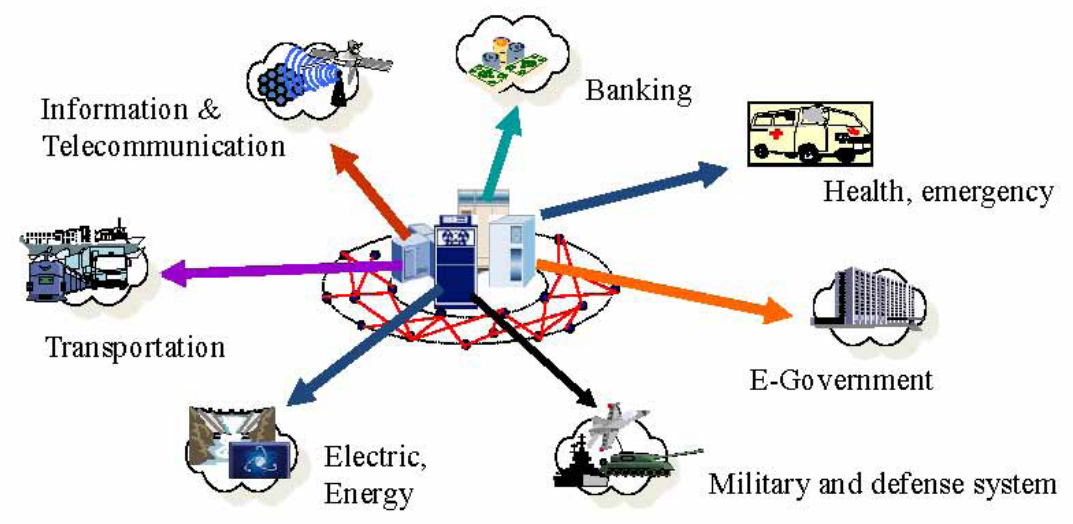
Critical infrastructure includes key systems, services and functions whose disruption or destruction would have a debilitating impact on the daily life of people, the economy, national security and public health and safety. The critical infrastructure consists of both physical elements (such as facilities and buildings) and virtual elements (such as systems and data, and information assets). The degree of "criticality" may be different from country to country, but it usually includes the following:[21]

- ICT (including telecommunications)
- Electricity generation, transmission and distribution
- Gas production, transport and distribution
- Oil and oil products production, transport and distribution
- Water supply (drinking water, waste water/sewage, stemming of surface water [e.g., dykes and sluices])
- Agriculture, food production and distribution
- Heating (e.g., natural gas, fuel oil, district heating)
- Public health care (hospitals, ambulances)
- Transportation systems (fuel supply, railway network, airports, harbours, inland shipping)
- Financial services (banking, insurance)
- Security services (police, military)
- Emergency, health and rescue services
- Public agencies and administration, justice system
- Media and major research establishments

Countries at all stages of cybersecurity development need to plan for and develop policies to protect what they determine to be their critical infrastructures in order to provide reasonable assurance of resilience and security to support national missions and economic stability.

21 Wikipedia, "Critical infrastructure". Available at http://en.wikipedia.org/wiki/Critical_infrastructure (accessed on 14 February 2012).

Figure 2. Examples of the critical infrastructure



3.1.2 Critical Information Infrastructure

The critical information infrastructure includes the systems, services, networks and functions that form a vital part of a nation's economy and society, either by providing essential goods and services or constituting the underpinning platform of other critical infrastructures. The critical information infrastructure includes the public telephone network, the Internet, and terrestrial and satellite wireless networks. They are regarded as critical information infrastructures since their disruption or destruction would have a serious impact on vital societal functions.

Many of the most critical systems are extremely vulnerable to natural disasters such as earthquakes, tsunami, extreme weather events, and so forth. Even when they are not physically impacted, sudden demand surges during crises can provoke blackouts, leading to loss or denial-of-service (DoS). Similar scenarios can occur through deliberate or accidental human action.

The critical information infrastructure has become especially vulnerable to attackers for fun seeking, intelligent, organized hackers, cybercriminals and terrorists. The main methods used to attack critical systems are malware (computer viruses, worms, logical bombs, Trojans) that modify and destroy information or block the computer systems. Other methods for eavesdropping on information exchange in computer networks as well as methods for modifying the normal function of the computer network and blocking the access to its services are also widely used for destructive purposes.

The followings are the major critical information infrastructure attacks:

- Unauthorized access to sensitive or confidential information stored or transmitted
- Destruction, modification or substitution of software needed by critical infrastructures
- Limited access for the agents able to prevent or mitigate the results of the attacks

The possible consequences from critical information infrastructure attacks include:

- Blocked transportation, electricity and water supply, communication, data transmission, nuclear power plant control and air traffic control
- Bankruptcy of commercial structures and financial systems, failure of international business transactions, destabilization of markets and financial institutions, money and information theft

- Loss of intellectual property or reputation
- Human victims or material losses, provoked by the destructive use of critical infrastructure elements (cybersabotage in the food industry, air or railway traffic)
- Unauthorized access and/or modification of personal information
- Possibility for imputing terrorist acts to other country/government and aggravation of the tension in international relations

3.2 A General Framework for the CIIP

3.2.1 Objectives of the CIIP

The CIIP has three strategic objectives:[22]

- Prevent cyberattacks against critical infrastructures
- Reduce national vulnerabilities to cyberattacks
- Minimize damage and recovery time from cyberattacks that do occur

In order to achieve these objectives a new strategy is needed that is based on a four-pillar model for the CIIP:[23]

- Taking preventive measures at all levels
- Improving early detection and warning and rapid reaction capabilities, both for damage control and pursuit of the culprits
- Limiting the impact of disruptions on government and society
- Ensuring that the affected systems continue to function at a minimum level or can be restored within the shortest possible time

And to implement these strategies, the essential tasks for the CIIP can be illustrated in a four-pillar model (see figure 3). The four pillars of this model are prevention and early warning, detection, reaction, and crisis management.[24]

Prevention is defined in the narrow sense as consisting of activities that promote the general preparedness of companies. This involves the dissemination of recommendations and guidelines on best practices, timely and credible warning of specific threats, and the implementation of training and exercises. It is worth noting that prevention and early warning cannot be approached on a purely technical level—potential dangers have to be weighed up constantly in a trade-off against risk situations.

22 Eugene Nickolov, "Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations", *Information and Security: An International Journal*, Vol.17, 2005, pp. 105-119. Available at http://www.comw.org/tct/fulltext/05nickolov.pdf (accessed on 10 January 2012).

23 Ibid.

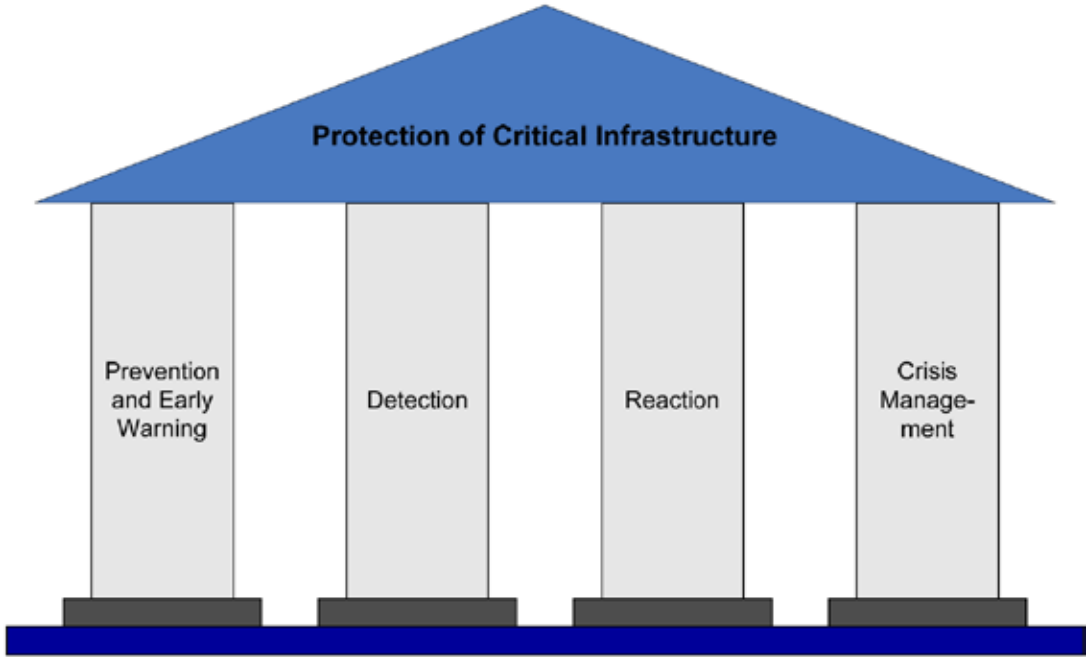
24 Manuel Suter, A Generic National Framework for Critical Information Infrastructure Protection (CIIP), ETH Zurich, Center for Security Studies, August 2007. Available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf (accessed on 10 January 2012). The subsequent paragraphs describing the CIIP four-pillar model draws heavily from this reference.

Detection is the second pillar. In order to promote security and to avoid particularly vulnerable technologies, it is crucial that new threats be discovered as quickly as possible. In order to recognize emerging threats on a timely basis, the CIIP unit depends on a broad national and international network.

Reaction includes the identification and correction of the causes of a disruption. Initially, the CIIP unit should provide technical help and support to the targeted company. But, the CIIP unit cannot take on the management of incident response for these companies.

Crisis management has been part of the CIIP since its inception. Depending on the organization of a state's crisis management administration, the CIIP unit can be positioned in several different ways. It should be well-positioned in order to have direct access to decision makers, because a key function of the CIIP unit is to alert the responsible people and organizations. In case of a national crisis, the CIIP unit must be able to offer advice directly to the government.

Figure 3. Four pillars of CIIP



source: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf

3.2.2 Measures for the CIIP[25]

3.2.2.1 The National Level

Five national priorities can be defined as follows:

1. Establish a national cyberspace security response system
2. Develop a national cyberspace security threat and vulnerability reduction programme
3. Create a national cyberspace security awareness and training programme

25 This sub-section is drawn heavily from Eugene Nickolov, "Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations".

4. Secure government systems

5. Strengthen national security and international cooperation on cybersecurity

The framework for the CIIP at the national level has to be considered in the wider context of the business, social and technical environment. The CIIP requires a multidisciplinary response incorporating technical, management and educational solutions. Both vendors and consumers need to prioritize better security in their products. Companies must adopt and share their best practices. Governments need to promote better understanding of computer security and ethics through public education efforts. It is also important to have improved communication and coordination at three levels—within the industry, between the industry and the government, and within governmental structures and bodies.

Protection of the Critical Information Infrastructure within Enterprises and among Industries[26]

Factors that contribute to critical infrastructure vulnerability in enterprises include:

- Large staff
- Numerous physical facilities
- Wide availability of phone numbers
- Lack of security training
- Lack of a system for data classification
- Lack of procedures for reporting and reacting to incidents

The measures that could be undertaken include:

- **Physical protection of key elements of the critical information infrastructure**. Depending on the business, it may be necessary to install badge swipes, access codes or hire security guards. Cable locks, alarms, motion detectors, anti-theft systems and biometric scanners are also useful. Electronic keypads on server rooms that are not shut off in the event of power loss may be necessary for some companies. These are just a few examples of physical security measures needed to secure a facility.

- **Technical measures – technical security**. They include the use of e-mail and file encryption to conceal the operations and prevent sensitive data, such as national security secrets, private customer account data or confidential proprietary information, from unauthorized disclosure. Firewalls, intrusion detection systems, access control lists, strong password policy, and anti-virus software are also components that organizations may need.

- **Social measures – staff training and control**. A background check on new employees is an excellent security measure. This is a good defence measure from an information warfare standpoint. It informs employers whom they are hiring before the new employee has any physical access to a facility and to sensitive documents. User training is a huge step in the right direction. All employees have to be trained to lock their computer screens when they leave their desks, to use strong password management schemes, to know the methods of social engineering so that they do not end up revealing any confidential information. When employees feel personally involved in protecting the company or agency they work for, they tend to take more pride in what they do. The more they understand the policies set forth, the less potential problems will arise in future.

26 Ibid.

- **Security policy**.[27] All technical and social measures have to be implemented with a strong security policy that should:
  - Define what the user wants to protect
  - Analyse what it is the user wants to protect it from
  - Explain how the user intends to protect it

  The policy must be updated regularly, signed off by management, and everyone in the information technology (IT) department must be familiar with it. The overall security policy will address such areas as:
  - Physical security of the data and systems
  - Access control to the data and systems
  - Data integrity and availability
  - Contingency and recovery plans

  To be effective, the security policy must be both inclusive and dynamic. To be successful, it must have realistic goals and be phrased in a way that is simple and short enough to ensure it is understood and followed by all users.

Public / Private Cooperation between Industry and Government

Due to the large number of private actors that own or use the critical information infrastructure, forming public-private partnerships is an important part of CIIP. These partnerships should include the following:

- Address the problems and threats to the national critical information infrastructure
- Include alerting software and hardware vendors to the security and protection of their products
- Fast and efficient reaction to all incidents related to the functioning of the critical systems
- Create systems for formal and informal sharing of information on computer related crimes and cyberterrorism

Looking into more detail at the last item, it is clear that the private sector and law enforcement must gather and share information about threats, vulnerabilities, remedies and successful operating models of cybersecurity. To improve CIIP, the private sector has to share some information about incidents and damages with the government and the public, even when the information shared is detrimental for the particular company disclosing the information. Only the complete disclosure of information both by the private sector and the government can even the playing field between the potential attackers and the defenders of the critical information infrastructure.

On the other hand, sharing details of the critical information infrastructure has some negative side effects both to public and private interests. Information sharing could raise privacy concerns, expose proprietary corporate secrets, and reveal weaknesses and vulnerabilities that erode public confidence and invite hackers. Retailers and credit card issuers often worry that disclosing any

27 Security policy is defined as the set of rules laid down by the security authority governing the use and provision of security services and facilities.

problems with the security of online transactions (e.g., hackers gaining access to credit card numbers or purchase history) may undermine public confidence in Internet commerce, to the detriment of their businesses. An Internet service provider (ISP) attack disclosure also could lead to a loss of customers and revenue. Releasing a top ten vulnerabilities list to the public helps system administrators and computer users, but provides hackers with the information they need to successfully attack at-risk networks. Therefore, trust with respect to how the information will be used, how it will be protected from disclosure, and whether legal tools can be used by the government and private parties against those sharing information is needed among those sharing information in order to achieve successful protection of the national critical information infrastructure.

Tasks at the Governmental Level

The most important task is the creation of a national security policy that includes the following:

- Security policy for strategic objects controlled by computer networks, based on the risk analysis of possible attacks
- Programmes for practical implementation of security policy and operational measures to ensure that the rules are followed
- Strict adherence to the assessment standards of products and systems prone to cyberattacks
- Analysis of the current reaction abilities of network elements and systems based on their reaction to possible attack scenarios
- Assessment of the efficiency of protection tools by –
  - Reliable verification (reasonable balance between confidentiality and access to common data)
  - Protection of all systems and subsystems using testing (e.g., honey pots and honey nets) and specific criteria (e.g., ISO/IEC Common Criteria)

One of the most important aspects of effective organization of the CIIP is government funding. Often, the security measures undertaken by businesses are not very effective—or effective enough to outweigh the investment. Government investments in R&D of computer security measures resolve this problem to a certain extent.

The second important task to be performed at the governmental level is the elaboration of common policy in the control of computer systems especially for the vital branches of national defence and business. This policy has to be founded on a legal framework for the CIIP to be considered in the larger context of the business, social and technical environment. The CIIP has to be seen as a part of society's (cyber) crime prevention. Cybercrime is a very broad concept that has various meanings, ranging from technology-enabled crimes to crimes committed against individual computers, and includes issues such as copyright infringement, computer fraud, child pornography and network security violations. Cybercrime is generally fought with traditional law-enforcement strategies that include adopting appropriate legislation and fostering international cooperation.

Only governmental institutions could create a united front against cyberattacks. This front needs a central unit for infrastructure protection—a body that is already created in some countries. It must focus on the collaboration of the private sector, law enforcement, prosecution and the intelligence community and provide support in the following four areas:

- Management of the CERT in the country
- Investigations on the Internet to identify criminal misuse and monitor dangerous situations, such as the vulnerability of widely used hardware and software products
- Verifying whether the reported matter constitutes a criminal offence, coordinating with ongoing proceedings and referring the case to the relevant prosecution authorities at home and abroad
- Analysing the interconnectedness of critical sectors and their dependence on ICTs, and developing measures for prevention, response and comprehensive security management of the national critical information structure

These tasks include systematic examination of all infrastructure areas for possible weaknesses and improvement possibilities in terms of IT dependencies and security. Further, they necessitate the appropriate solutions, recommendations for each individual sectors, as well as indications of technical or organizational support needed in order to be executed.

The USA was the first country to broadly address the new vulnerability of the vital infrastructures. The Presidential Commission on Critical Infrastructure Protection (PCCIP) defined in 1997 the critical information infrastructure, its particularities and vulnerabilities. Following the PCCIP's publication, then US President Bill Clinton started initiatives to increase the protection of critical infrastructures in the USA on the premise that a joint effort by government, society, organizations and critical industries was needed to defend these vital assets.

Recently, following the example of the USA, many countries including Australia, Canada, Germany, Japan, the Netherlands, Norway, Switzerland and the UK have taken steps to better understand the risks to their critical information infrastructure, and have proposed measures for the protection of these assets.

CERT coordination centres are also being established around the globe and provide assistance in handling computer security incidents and vulnerabilities, publishing security alerts, researching long-term changes in networked systems, and developing security information and training materials.

3.2.2.2 International Level

Critical information infrastructure attacks are becoming a growing transnational phenomenon, making prosecution extremely difficult. Therefore cybersecurity must be approached from an international perspective, taking into account:

- National and international initiatives
- Legal developments
- Best practices and resources
- Guidance on developing and implementing effective security programmes
- Technological considerations

Achieving cybersecurity requires a global effort; it cannot be achieved by a few nations.

It requires the input from all ICT users, including citizens, governments, businesses and organizations. On the multinational front, the Group of Eight (G8), the Asia-Pacific Economic Conference, the European Union (EU), the Council of Europe, the Organization of American

States, the Organisation for Economic Co-operation and Development (OECD), and the United Nations are each working towards solving this problem. As early as December 1998 the General Assembly of the United Nations approved Resolution 53/70 on cybercrimes, cyberterrorism and cyberwar.[28] It appealed to the member States to inform the United Nations Secretary-General of their opinions on the following issues:

- The problems related to information security
- Basic notions related to information security
- Development of international principles of the global information space and telecommunications, which help combat cyberterrorism and cybercrimes

The EU has adopted the Proposal for a Council Framework Decision on Attacks against Information Systems[29] that recommends a harmonized approach to attacks against information systems through uniform prohibitions against illegal access to information systems, as well as instigating, aiding or abetting such acts. The Council of Europe developed the Convention on Cyber Crime (with the USA participating as an observer), which has since been signed by 42 countries.[30]

3.3 Case Studies

3.3.1 Republic of Korea

The Korean CIIP policy is embodied in the Korean CIIP Act enacted and promulgated in January 2001. The CIIP Act was partially revised in November 2007. Under this Act the Committee on the Protection of the Critical Information Infrastructure was established to coordinate the tasks of establishing and executing the critical information infrastructure policies of the relevant ministries and institutes for the purpose of efficient information protection on a government-wide basis.

After the hacking incidents that targeted some of the major government organizations in 2004, the government undertook to develop a strong and integrated management system on a government-wide basis for quick response and incident handling against cyberterror. The "National Cyber Security Management Regulations" (Title 141, 2005.1.31) were enacted to reform the basic structure of national cybersecurity.

The NCSC coordinates the efforts of relevant departments and agencies. In the field of cybercrime investigation and prevention, the Internet Crime Investigation Center under the authority of the Supreme Public Prosecutors' Office plays a central role. The Electronics and Telecommunications Research Institute is taking the lead in developing technology and providing support to protect critical information infrastructure.

In 2008, the Ministry of Information and Communication (MIC) was abolished and its functions in the area of information security were transferred to KCC, MOPAS and the Ministry of Knowledge Economy. Together, they are sharing CIIP-related responsibilities.

28 United Nations General Assembly Resolution/Decision 57/53, Development in the field of information and telecommunications in the context of international security, Report A/57/505. Available at http://unhq-appspub-01.un.org/UNODA/Vote.nsf/91a5e1195dc97a630525656f005b8adf/a8d9313a2542cfdd85256c460052c049?OpenDocument&ExpandSection=4 (accessed on 10 January 2012).

29 EU, Proposal for a Council Framework Decision on attacks against information systems. Available at http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&lg=en&numdoc=52002PC0173 (accessed on 10 January 2012).

30 Council of Europe, Convention on Cybercrime. Available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG (accessed on 10 January 2012).

MOPAS, KCC and the Korea Internet Security Center (KISC; Korea Computer Emergency Response Team Coordination Center [KrCERT/CC]) within the Korea Internet and Security Agency (KISA)[31] are undertaking efforts to foster a culture of safe Internet and telecommunications networks.

As a public-private partnership, the National Information Security Alliance strives to improve information security by fostering information exchange between governmental agencies, enterprises and research institutes. The Financial Information Security Alliance has members from banks and insurance companies and strives to implement international information protection policies.

The Information Security Practice Alliance is an initiative fostering information protection activities in the private sector, and the Korea Information Security Industry Association is an exchange platform for the information security industry.

3.3.2 Australia

In 2010, the Australian government launched the Critical Infrastructure Resilience Strategy.[32] This Strategy describes the Australian government's approach to enhancing the resilience of the critical infrastructure to all risks—from natural disasters, to equipment failure and crime. The strategy promotes a resilient approach to ensure the continued operation of critical infrastructure in the face of all threats and hazards. This approach focuses on the country's ability to adapt to change, reduce exposure to risk and learn and bounce back from any type of threat or hazard.

As a significant proportion of Australia's critical infrastructure is privately owned or operated on a commercial basis, the strategy not only outlines the various activities undertaken by the Australian government, but also includes how it engages with business, community and individuals. The Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience[33] was established as its primary mechanism to build a partnership approach between business and government for critical infrastructure resilience.

Promoting cybersecurity is one of the six strategic imperatives of the strategy—"to maintain a secure, resilient and trusted electronic operating environment, including for critical infrastructure owners and operators." The Information Technology Security Expert Advisory Group (ITSEAG) provides advice to the TISN on emerging IT security issues that will impact on Australia's critical infrastructure sectors. The ITSEAG membership consists of IT security experts from industry, Australian academia and the Australian government.[34]

The strategy builds on the previous Critical Infrastructure Protection Program and has been developed with key stakeholders, including Critical Infrastructure Advisory Council members, state and territory governments, as well as owners and operators of critical infrastructure.[35]

A separate implementation plan will be developed that will describe, in detail, how the Australian government plans to execute the strategy. Development of the implementation plan will be developed in consultation with business and government stakeholders.

31 http://www.kisa.or.kr/eng/main.jsp.

32 Australian Government, Critical Infrastructure Resilience Strategy, 2010. Available at http://www.tisn.gov.au/Pages/default.aspx (accessed on 14 February 2012).

33 http://www.tisn.gov.au.

34 TISN, "Cyber security". Available at http://www.tisn.gov.au/Pages/Cyber_security.aspx (accessed on 14 February 2012).

35 "New critical infrastructure resilience strategy for Australia", *Homeland Security News Wire*, 12 July 2010. Available at http://www.homelandsecuritynewswire.com/new-critical-infrastructure-resilience-strategy-australia (accessed on 14 February 2012).

3.3.3 Japan

The Information Security Policy Council (ISPC) and the National Information Security Center (NISC) play important roles in CIIP for the Japanese government. The ISPC is the central decision-making body for formalizing information security-related policy measures. It has been established under the IT Strategic Headquarters since 30 May 2005. The NISC is the operational arm of the ISPC and is responsible for the central coordination of information security issues in the Japanese government. The NISC has been established in the Cabinet Secretariat of the Japanese government since 25 April 2005.

The ISPC formulated the First National Strategy on Information Security on 2 February 2006 as the mid- to long-term national strategy with an overview and basic principles of information security issues.

The term for this strategy was three years from 2006 to 2008. The ISPC also formulated "Secure Japan 2006" on 15 June 2006 as a promotion plan for each fiscal year based on the mid- and long-term strategy. During these three years, the government strengthened various relevant measures based on the National Strategy in order to establish a "new public-private partnership model" with all entities appropriately playing their roles.

In protection of the critical information infrastructure, the ISPC formulated the Action Plan on Information Security Measures for Critical Infrastructures on 13 December 2005. The Action Plan addressed the rapid spread of IT usage and increasing IT dependence in the critical infrastructure sectors as well as growing interdependence among the critical infrastructure sectors.

This Action Plan, a sector plan of the National Strategy, identified 10 targeted critical infrastructure sectors—information and communication, finance, civil aviation, railways, electricity, gas, governmental/administrative services, medical services, water works, and logistics—to ensure a high level of information security. The Action Plan identified the causes of IT malfunctions that could interrupt services and reduce the function of critical infrastructures, which included not only intentional cyberattacks but also unintentional (accidental) factors and (natural) disasters.

3.3.4 United States of America

The Homeland Security Presidential Directive 7 established the US national policy for identification of and prioritization for protection of critical infrastructure. Signed by George W. Bush on 17 December 2003 it modified previous policy for a post-9/11 country.[36]

The directive defines relevant terms and delivers 31 policy statements. These policy statements define what the directive covers and the roles various federal, state and local agencies will play in carrying it out. The directive also identifies critical infrastructure sectors and key resource categories that the public and private sectors must work jointly to protect. It includes protection of the IT sector and the cross-sector cyberinfrastructure within all the sectors.

36 Wikipedia, "Homeland Security Presidential Directive 7". Available at http://en.wikipedia.org/wiki/Homeland_Security_Presidential_Directive_7 (accessed on 14 February 2012).

Summary

- The concept of the CIIP: To protect the virtual component of the CIIP, which is systems that provide the resources upon which all functions of society depend upon.
- CIIP vulnerabilities: Unauthorized access to sensitive or confidential information, destruction, modification or substitution of software needed by critical infrastructures, and limited access for the agents to prevent or mitigate the results of the attacks.
- CIIP objectives: Preventing cyberattacks against critical infrastructures, reducing national vulnerabilities to cyberattacks, minimizing damage and recovery time from cyberattacks that do occur.
- Four tasks for CIIP: Prevention and early warning; detection, reaction, and crisis management.
- Countermeasures that could be taken at the national level and international level for the CIIP.

This chapter can help policymakers establish CIIP policies and strategies to implement them.

4. ELECTRONIC AUTHENTICATION

You will find in this chapter discussions on:

- **The concept of electronic authentication and public key infrastructure (PKI)**
- **How to establish the national PKI infrastructure; and**
- **Case Studies from the Republic of Korea and Luxembourg for PKI best practices.**

4.1 Overview

As online business is rapidly increasing on the Internet, the remote authentication of users is critical. Electronic authentication provides a certain level of assurance regarding whether someone or something is who or what it claims to be in the cyberenvironment.[37] Thus, electronic authentication plays a critical role in the establishment of trust relationships for electronic transaction services, electronic government services and many other social interactions online. It is also an essential part of any method to protect information systems and networks, financial data, personal information and other information assets from unauthorized access or identity theft. Electronic authentication is therefore needed for establishing accountability online.

The methods in which someone may be authenticated fall into three categories, based on what are known as the factors of authentication: something you know, something you have, or something you are. Each authentication factor covers a number of elements used to authenticate or verify a person's identity prior to being granted access, approving a transaction request, signing a document or other work product, granting authority to others, and establishing a chain of authority.

Security research has determined that for a positive identification, elements from at least two, and preferably all three, factors be verified. The three factors (classes) and some of the elements of each factor are as follows:[38]

- The **ownership factors**: Something the user **has** (e.g., ID card, one-time password [OTP] token, security token, software token, phone or mobile phone)
- The **knowledge factors**: Something the user **knows** (e.g., a password, pass phrase, personal identification number [PIN], challenge response [the user must answer a question])
- The **inherence factors**: Something the user **is** or **does** (e.g., fingerprint, retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature, face, voice, unique bio-electric signals, or other biometric identifier).

4.2 Public Key Infrastructure

The PKI is a technical infrastructure for electronic authentication services. There are two types of cryptographies: a symmetric cryptosystem and asymmetric cryptosystem.

In symmetric (or secret key) cryptography, the same secret key is used to both encrypt message (plaintext) and decrypt a ciphertext. Symmetric cryptosystems require parties (sender and receiver) to share a unique secret key as initial arrangement. The secret key must be distributed to the parties through secure means because knowledge of the enciphering key implies knowledge of the deciphering key and vice versa.

In an asymmetric (or public key) cryptography system, there are a pair of keys (a public key and a private key). Public keys can be made widely public but the private key must always be kept secret. The private key is usually stored on a smart card or on a key token. The public key is generated from the private key and, although these keys are mathematically related, there is no feasible way to derive the private key from the public key. To send confidential data to someone securely using public key encryption, the sender encrypts the message with the recipient's public key. The recipient decrypts it with their corresponding private key.

37 Julia H. Allen et al., *Software Security Engineering: A Guide for Project Managers* (Addison Wesley, 2008).

38 SecurIT, "Strong Authentication". Available at http://www.securit.biz/standard.asp?strong_authentication (accessed on 10 January 2012).

Public key encryption can also be used to generate a digital signature to data, which is used to confirm that a document or message originated with the entity who claims to be the sender (or originator). The digital signature is actually a digest of the data that is produced using the signer's private key and appended to the message. The recipient uses the signer's public key to confirm the validity of the digital signature. In some public key systems, two public/private key pairs are used—one for encryption/decryption and another for digital signature/verification.

The components of the PKI are illustrated in figure 4.

Figure 4. Components of a PKI

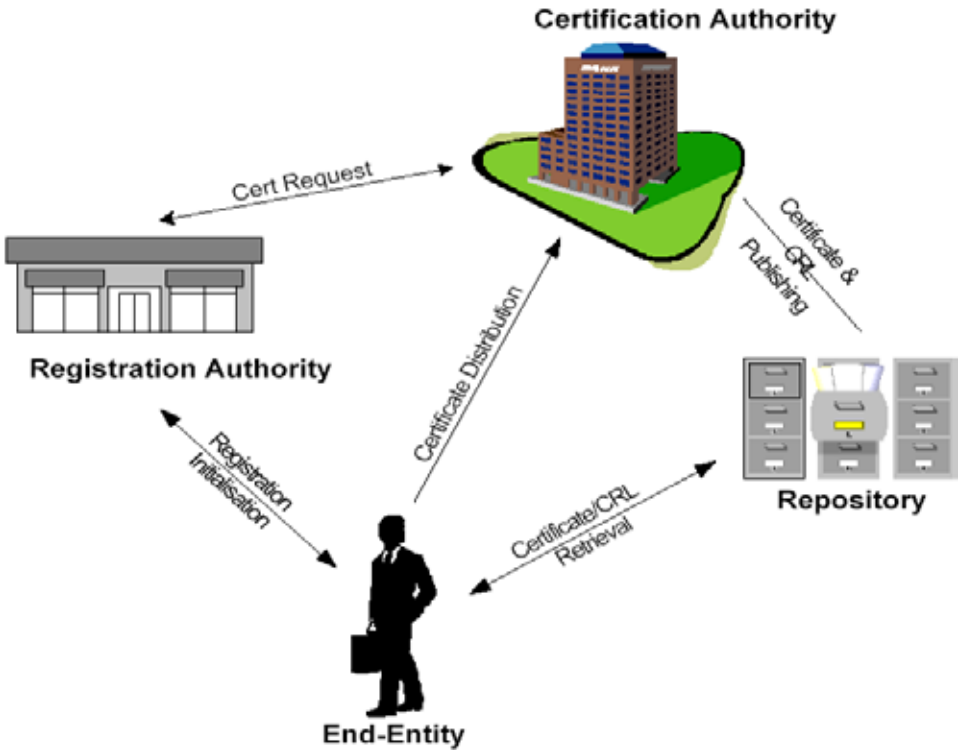


Figure 4 describes the components of the PKI: a certification authority (CA), a registration authority, an end-entity and a repository. A public key certificate is the digital equivalent of an ID card used in conjunction with a public key encryption system, also called a "digital ID", "digital identity certificate", "identity certificate" and "public key certificate". Digital certificates that are issued by a trusted third party are known as the CA. The CA issues and revokes certificates for other entities. The certificate is the data structure signed by a CA binding a public key to a specific end-entity.

The registration authority supports the function of the CA and performs tasks such as end-entity registration and identification. An end-entity is an owner of a public/private key-pair, subject of the certificate. The repository is a component used for publication and distribution of certificates and revocation information.

The internationally recognized standardized format for public key certificates is defined in Recommendation ITU-T X.509. In short, an X.509 public key certificate comprises a public key, an identifier of the asymmetric algorithm the key is to be used with, the name of the key pair owner, the name of the CA attesting to this ownership, the serial number and validity period of the certificate, the X.509 version number that this certificate conforms to, and an optional set of extension fields that hold information about the certification policy of the CA.

The whole certificate is then digitally signed using the private key of the CA. An X.509 certificate can be widely published, for example on a website, or in a Lightweight Directory Access Protocol (LDAP) directory. The CA's signature ensures that its contents cannot be modified without being detected.

In order to be able to confirm the validity of a user's public key certificate, a person needs to have access to the valid public key of the CA that issued the certificate in order to verify the CA's signature on the certificate. A CA may have its public key certified by another (superior) CA, so that validating public keys may involve a chain of certificates, which ends at the root CA. Root CA public keys are distributed as self-signed certificates (in which the root CA is attesting that this is its own public key). The signature allows a person to validate that the key and CA name have not been tampered with since the certificate was created. However, the name of the CA embedded in a self-signed certificate cannot be taken at face value, since the CA inserted the name in the certificate itself. Thus, a critical component of a PKI is the secure distribution of root CA public keys (as self-signed certificates), in a manner that can assure users that the public key really does belong to the root CA named in the self-signed certificate. Without this, one cannot be sure that someone is masquerading as the root CA.

4.3 Steps for Establishing a National Digital Signature Infrastructure

This sub-section describes the procedure for establishing the national digital signature infrastructure. There are four general steps as follows:

1. Establishing a Digital Signature Act
2. Determining the organizational structure for national PKI
3. Developing the certification policy and certification practice statement that can be used by the CAs
4. Performing a periodic or on-demand audit for the CA to check if they comply with the legal requirements of the Digital Signature Act

The first step would be to establish the digital signature law. The purpose of the Digital Signature Act is to establish the legal framework in order to promote the reliability of the digital message and their use. The digital signature law may include the following:

- Purpose of the law
- Terms definition
- Designation of licensed CA, if necessary
- Authorized certificates including issuance of certificates
- Operation of certification system
- Adoption of digital certification policy

The second step would be to determine the organizational structure of PKI. There are several types of PKI structure: hierarchical structure, mesh structure, bi-lateral cross-certified structure and bridge structure.[39]

A hierarchical PKI is one in which all of the end entities and relying parties use a single "root CA" as their trust anchor. If the hierarchy has multiple levels, the root CA certifies the public keys of intermediate CAs (also known as subordinate CAs). In a typical mesh style PKI, each end entity trusts the CA that issued its own certificate(s). Thus, there is no "root CA" for the entire PKI. The CAs in this environment have peer relationships; they are neither superior nor subordinate to one another. In a mesh, CAs in the PKI cross-certify, that is, each CA issues a certificate to, and is issued a certificate by, peer CAs in the PKI. In a bi-lateral cross-certified structure, PKIs can be connected via cross-certification to enable the relying parties of each to verify and accept certificates issued by the other PKI. If the PKIs are hierarchical, cross-certification will typically be accomplished by each root CA issuing a certificate for the other PKI's root CA. Another approach to the interconnection of PKIs is the use of a "bridge" certification authority (BCA). A BCA is a nexus to establish trust paths among multiple PKIs. The BCA cross-certifies with one CA in each participating PKI. Each PKI only cross-certifies with one other CA (i.e., the BCA), and the BCA cross-certifies only once with each participating PKI. As a result, the number of cross certified relationships in the bridged environment grows linearly with the number of PKIs whereas the number of cross-certified relationships in mesh architectures grows exponentially.

The simplest way to determine the organizational structure would be to use a hierarchical structure described above.

The third step is to develop and make publicly available the certification policy and certification practice statement that can be used by the CAs. The certification practice statement is a public statement that describes the practices a CA uses for issuing, renewing, revoking and validating digital certificates and for supporting reliance on certificates. The statement expands on the certification policies of a particular CA. It should be a detailed and comprehensive technical and procedural document that regards the operation of the supporting infrastructure.

The next step would be to perform a periodic or on-demand audit for the CA to check if they comply with legal requirement of the Digital Signature Act.

4.4 Case Studies[40]

4.4.1 Republic of Korea

The Korean PKI strategy is based on a dual public and private sector PKI for the provision of digital credentials to individuals. In this context, since 1999 the Korean PKI Strategy encourages the use of digital credentials based on PKI. The promotion of digital credentials by the governments is based on:

- Two PKIs: the national PKI that enables the use of digital certificates for private sector transactions, and the government PKI for transactions within the public sector.

39 M. Cooper, et. al, "Internet X.509 Public Key Infrastructure: Certification path building", RFC 4158, September 2005. Available at http://www.ietf.org/rfc/rfc4158.txt. The subsequent paragraph on the different types of PKI structure is drawn from this reference.

40 This sub-section is drawn heavily from: Laurent Bernat, "National Strategies and Policies for Digital Identity Management in OECD Countries", OECD Digital Economy Papers No. 177, 31 March 2011. Available at http://www.oecd-ilibrary.org/science-and-technology/national-strategies-and-policies-for-digital-identity-management-in-oecd-countries_5kgdzvn5rfs2-en (accessed on 10 January 2012).

- The recommendation to use digital certificates for any financial services such as Internet banking, online stock trading and online shopping transactions that are above USD 260.

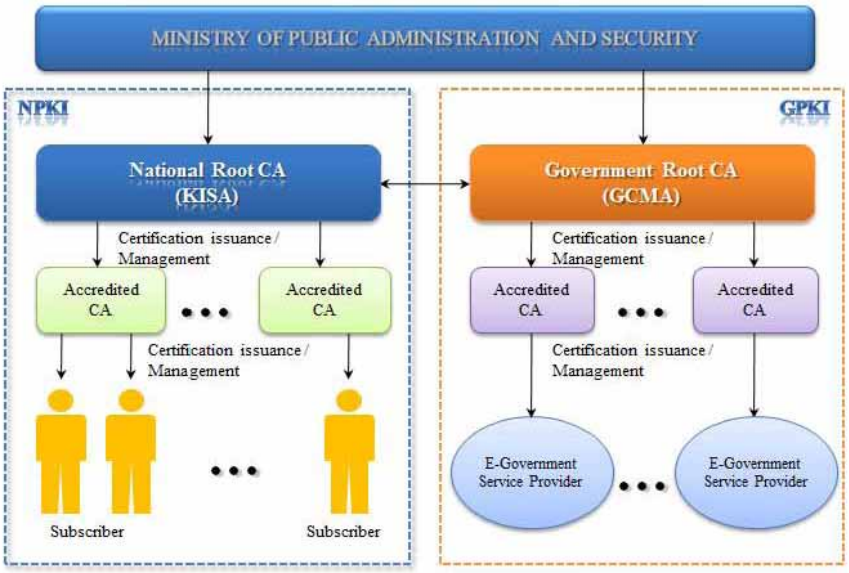
The strategy is based on a legislative framework including the 1999 Electronic Signature Act that sets forth a framework for the use of electronic identity credentials for e-commerce and electronic documents, and the 2002 e-Government Act for the promotion of governmental digital certificates.

The structure of the national PKI is hierarchical, comprising of a Root CA, accredited CAs and the users. National PKI certificates are issued by five private sector accredited CAs, and the government PKI certificates are issued by MOPAS. KISA plays the role of the root CA. National PKI certificates are provided for free when used in a specific area (e.g., e-commerce, banking, stocks). All-purpose certificates are provided for a small annual fee of USD 4. While the Government Certification Management Authority acts as root CA in public areas, the Korea Local Information Research and Development Institute provides government PKI certificates to civil servants. The number of digital certificates delivered is 23.6 million as of October 2010.

The Republic of Korea developed the Certificate Trust List (CTL) mechanism to enable interoperability between national public key infrastructure (NPKI) for the private sector and government public key infrastructure (GPKI) for the governmental sector. In operation since 2002, this system did not raise particular technical problems but it was difficult to establish and in particular it took a long time to reach an agreement regarding aspects such as who will operate the CTL and how to renew an electronic certificate based on the PKI with the CTL system.

The Republic of Korea encourages the interoperability of electronic identity credentials by monitoring the root CA and accredited CAs to make sure they comply with interoperability requirements. The Electronic Signature Act was modified to introduce an obligation for private sector to comply with the national PKI standard. Twenty-four norms for safety and reliability of a PKI certificates have been adopted.

Figure 5. Two PKI domains of the Republic of Korea



4.4.2 Luxembourg

The current digital identity management strategy of Luxembourg aims to increase security in e-commerce and e-government transactions. It is based on PKI certificates delivered by LuxTrust, a CA established in 2005 on the basis of a public-private partnership between the government and key business actors such as financial institutions. The status of LuxTrust enables close cooperation with financial institutions and is overseen by the official financial supervisor (Commission de Surveillance du Secteur Financier). LuxTrust provides PKI certificates on smart cards and USB tokens. It also provides "signing server certificates" that generate one-time passwords either via SMS messages or by using a dynamic authentication token. Registration requires a face-to-face relationship with one of the banks recognized by LuxTrust as registration authorities.

The PKI certificates enable access to public and private sector online applications and digital signature of documents and e-mail. With LuxTrust PKI certificates, individuals can log in to a unique counter for citizen-to-government interactions called "de Guichet" to carry out a large number of formalities online. Private sector services using LuxTrust certificates are mainly offered by banks and financial institutions.

The strategy relies on a centralized registration policy based on a central register, a unique identification number and a mandatory paper-based identity card. Future plans include the distribution of national identity cards containing embedded electronic data, including biometrics, to be used for public and private sector digital interactions.

Summary

- The concept of electronic authentication: The process of establishing confidence in user identities electronically presented to an information system. The methods in which someone may be authenticated fall into three categories, based on what are known as the factors of authentication: something you know, something you have, or something you are.
- The PKI is a technical infrastructure for electronic authentication services. The concept of public key algorithms: A public key can be made widely public but a private key must always be kept secret; the sender encrypts the message with the recipient's public key, and the recipient decrypts it with their corresponding private key.
- The components of a PKI: A CA, a registration authority, an end-entity and a repository.
- Steps for establishing a national PKI: Establishing the digital signature act, determining the organizational structure for a national PKI, developing the certification policy and certification practice statement that can be used by the CAs, and performing a periodic or on-demand audit for the CA to check if they comply with legal requirements of the digital signature act.

This chapter can be used when policymakers set up the authentication policy and implement the PKI scheme for their countries.

5. NATIONAL INCIDENT MANAGEMENT

You will find in this chapter discussions on:

- **The concept of national incident management;**
- **The incident handling flow;**
- **Assessment of the incident through classification on the seriousness of the incident;**
- **The process of establishing a national incident management system;**
- **The steps to establish a national CERT; and**
- **Case Studies on the legal framework, policies and strategies for national incident management from Finland and the Republic of Korea.**

5.1 Overview

The formulation and implementation of a cybersecurity strategy requires a comprehensive approach that involves the adoption of appropriate legislation against the misuse of ICTs for criminal purposes. It also requires coordinated action to prevent, prepare, respond and recover from incidents in cooperation with relevant partners at national, regional and international levels. Most of these missions are performed by so-called CERTs.

A CERT is defined as a service organization responsible for receiving, reviewing and responding to computer security incidents. It provides the necessary services to handle them and support their constituents to recover from breaches.

There are two types of CERTs—a private CERT and a public CERT. Private CERTs are responsible for computer security incidents within a company or their customers (e.g., BT CERT [http://www.btcert.bt.com]). Public CERTs take care of computer security incidents within the government institutions, and sometimes also receive complaints from the general public. The proactive services are playing a very important role.[41]

There can be more than one CERT in a country serving the interest of various constituencies for example the academic, banking sectors, military and within an organization. These CERTs are focused on and provide services and support to their defined constituency for the prevention of, handling and response to cybersecurity incidents. However, it is also possible for a country to designate a national CERT to serve government or government-related organizations. A national CERT is a national focal point within a country or region to coordinate incident handling activities.

The international cooperation between the different types of CERTs from different countries and regions is becoming essential in IT security activity. Usually, there are very close relations between the present CERTs. Newly established CERTs can benefit from these close ties and draw from the experience and expertise already gained.

5.2 Incident Handling Flows[42]

A crisis is said to pass through three phases:

- The pre-phase occurs when there are indications that something may go wrong. In this phase, an organization should be on alert and raise its preparedness level.
- The emergency and handling phase is when the crisis occurs. An emergency is often unexpected and ill-timed, and frequently occurs during non-business hours or weekends. As every crisis is different, the handling should not be performed according to some standard routine that states every action to be taken regarding a defined threat.
- After-phase, follow-up phase or aftermath, is the phase that is crucial if the organization is going to resolve the crisis and survive. This phase consists of several other sub-phases such as psychological first aid, actions to get back to business, lessons learnt, and so forth.

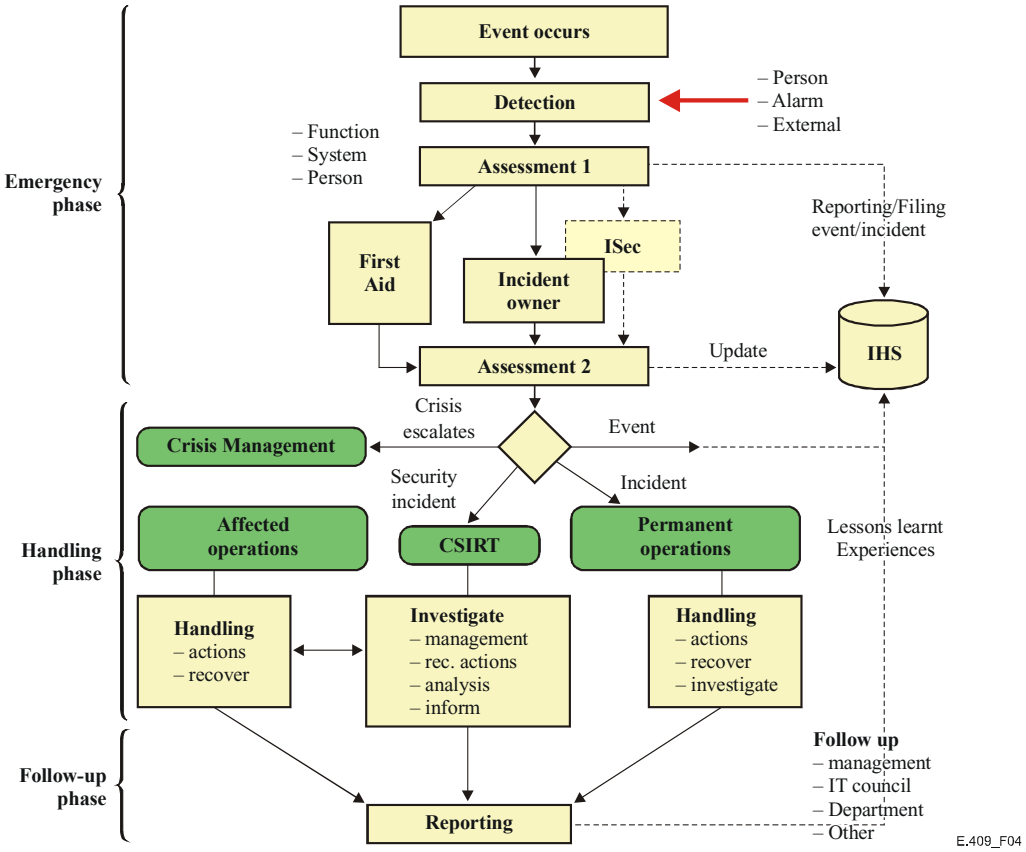
41 See http://www.bsi.bund.de/certbund.

42 This sub-section is drawn heavily from: ITU, “Incident organization and security incident handling: Guidelines for telecommunication organizations”, ITU-T Recommendation E.409, May 2004.

Figure 6 shows an incident flow for the emergency and handling phase, and the follow-up phase.

Under normal circumstances, the handling of an incident does not reach crisis management level. If an incident should be transferred to crisis management, it means the incident has escalated into a crisis.

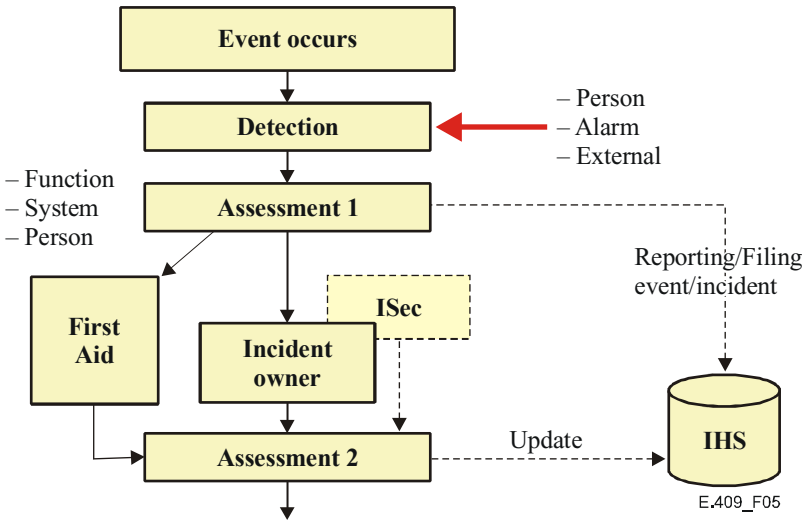
Figure 6. Incident flow



Source: ITU, "Incident organization and security incident handling: Guidelines for telecommunication organizations", ITU-T Recommendation E.409, May 2004, p. 6.

The emergency phase may be compared with an accident situation, that is, during a traffic accident the first actions taken are often critical in terms of the final outcome. These actions have the most important consequences in terms of the outcome. See figure 7 for the stages in the emergency phase.

Figure 7. The emergency phase in the incident flow



Source: ITU, "Incident organization and security incident handling: Guidelines for telecommunication organizations", ITU-T Recommendation E.409, May 2004, p. 7.

An event may be detected visually by an individual, for example, by tracking an error message, reading a result file or by audit control. Visual detection may occur when the operator sees someone committing an intrusion or when someone detects a fire. An event can also be detected by a person who has a feeling that something is wrong, that something unusual is going on.

Logical alarms are situations that call for the attention of the end-user, operating personnel, security functions and so on. A logical alarm can be an alarm triggered by the anti-viral software, the audit subsystem or the firewall and intrusion detection system. An event can also trigger physical alarms such as fire alarms and burglar alarms.

External detection occurs when someone not belonging to the organization detects the event. This can be, in the worst case, announced on the news, or a reporter who investigates sources or contacts the organization to obtain a comment regarding an event the organization has not yet detected. It can also be the law enforcement authorities who notify the security department during the investigation of a crime, or a righteous citizen discovering an undesired feature of the telecommunications organization's website.

When an event is detected, an initial assessment of the situation must be made in order to confirm the category and seriousness. This is done by categorizing the event by type, that is, either as an incident, a security incident, a crisis, or just an event. After that, the scope and consequences have to be considered.

Table 1 describes a simple classification of the events, applied for security incidents only, to use when determining the seriousness of an incident or security incident. Table 2 illustrates the typical example of seriousness and classification according to incident types.

Table 1. Classification of events based on their seriousness

Class 4	Very serious	• A security incident that has significant consequences for the organization, e.g., coordinated attacks, computer intrusions, and theft of sensitive and confidential information. • A security incident that falls within this class requires significant countermeasures and results in significant damage.
Class 3	Serious	• A security incident that has consequences for the organization, e.g., computer sabotage, computer fraud, breach of integrity, misuse or exposure of corporate or customer information.
Class 2	Less serious	• A security incident, such as intrusion attempts, misuse of computing resources, etc. • A security incident that falls within this class has less consequence, requires minor countermeasures and results in little damage.
Class 1	No consequences	• An incident that is handled by the permanent organization but may be escalated to a security incident, e.g., scans, single viruses, abusive events, and attacks directed to mail systems. This class usually comprises incidents that affect the normal production. • A security incident that falls into this class requires minor or no countermeasures and results in little or no damage.

Table 2. Examples of seriousness and classification according to specific incident types

	No consequences	**Less serious**	**Serious**	**Very serious**
E-mail	Spam (blocked by spam filter)	Fraud (phishing)	Targeted attack (spear phishing)	
Computer intrusion	Failed attempt	Single access (user compromise)	Multiple access (user compromise), Single access (application, root compromise)	Mass access (application, root compromise)
Denial-of-service		Annoyance (scratch the surface)	Disturbance (throughout impact)	Unavailability (stop in service)
Malware	Single known	Single known	Multiple infections	Mass infections

Source: ISO/IEC FCD 27035, Information technology – Security techniques – Information security incident management, 2010.

This assessment of the seriousness of an event can be made by the person who detects the event, who can also choose to report the detected event to a function, for example, the helpdesk or Information Security Department. When an event is reported to a function, it becomes the responsibility of that function. The functions that may receive a report of detection are also called Point-of-Contact (POC), and they are responsible for handling the situation. An alarm is normally automatically transferred to the responsible person, function or system. All reported events should be registered in an incident handling system.

A POC is a unit or a person to whom an event is reported. An event cannot be reported to the CSIRT as this is a virtual group that is formed at the time of a security incident. A security incident can be reported to the Information Security Department that is responsible for the CSIRT, or any other POC where the correct assessment will be made and contact initiated with the responsible units.

All functions and units that may receive an alarm or indication of an event must be given instructions on how to act. This must be done to avoid events and alarms being neglected or incorrectly handled.

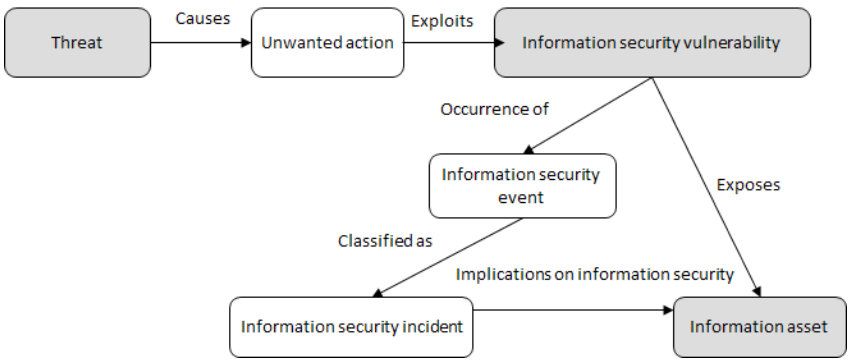
5.3 Incident Handling in an Organization[43]

An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant. An information security incident is single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

The occurrence of an information security event does not necessarily mean that an attempt has been successful or that there are any implications for confidentiality, integrity and/or availability, that is, not all information security events are classified as information security incidents.

Figure 8 illustrates the relationship of objects in an information security incident chain. A threat acts in unwanted ways to exploit the vulnerabilities (weaknesses) of information systems, services or networks, which is the occurrence of information security events and potentially causes unwanted incidents to information assets exposed by the vulnerabilities.

Figure 8. Relationship of objects in an information security incident chain

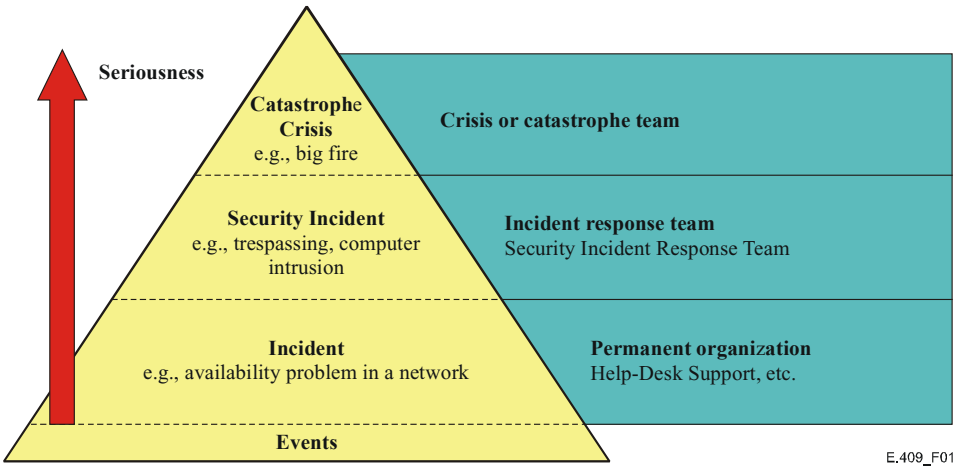


Source: ISO/IEC FCD 27035, Information technology – Security techniques – Information security incident management, 2010.

43 This sub-section is drawn heavily from: ITU, "Incident organization and security incident handling: Guidelines for telecommunication organizations", ITU-T Recommendation E.409, May 2004.

A security incident is a security breach, threat, weakness and malfunction that may have an impact on the security of organizational information assets. In general, an incident is less severe than a security incident and an information security incident is a particular type of security incident. The event can be classified into incident, security incident and crisis depending on the seriousness of impact as shown in figure 9.

Figure 9. Pyramid of events



Source: ITU, "Incident organization and security incident handling: Guidelines for telecommunications organizations", ITU-T Recommendation E.409, May 2004.

The closer to the top an event is located, the more serious. The event is an observable occurrence that is impossible to (completely) predict or control. The incident is an event that may lead to an occurrence or an episode that is not serious. The security incident is any adverse event whereby some aspect of security can be threatened.

To protect the organization assets, the organization should implement three protection mechanisms: preventive mechanisms, detection mechanisms and reacting mechanisms. The protection mechanisms should reflect the requirements of its security policy, including legal compliance. The incident handling organization and its tasks should support these requirements.

An organization should implement all the steps involved in protective security mechanisms in order to obtain coherent protection. The preventive protection mechanisms come first. When adequate preventive protection mechanisms are in place, implemented via physical or logical protection, an organization should identify and activate the detecting protection mechanisms. The detection protection mechanisms could, in the simplest form, be the checking of log files and logical or physical alarms (e.g., burglar alarms, fire alarms or other surveillance functions).

One form of detection mechanism is the intrusion detection system. Once an incident is detected, action should be taken. Such action usually comprises the following tasks:

- Stop an ongoing incident
- Identify the scope/scale of the incident
- Limit the damage
- Take measures in order to investigate the course of events
- Prevent the incident from recurring

As part of the reacting mechanism, actions necessary to stop and limit the incident (contain it) and prevent re-occurrence are performed by the permanent organization. If the incident escalates into a crisis, a specially trained crisis group performs the actions. The incident response team should investigate and analyse the incident.

After all these three protection mechanisms are in place and functioning, there is a deterrent effect, that is, the perpetrator knows there are functioning protection mechanisms and that detection and reaction to incidents are prompt. The deterrent effect can be increased by reacting to all incidents and by reporting any illegal incidents to law enforcement authorities. Refer to Annex for more details.

5.4 Establishing a National Incident Management System[44]

It is important for the government to create or identify a national organization to serve as a focal point for securing cyberspace and the protection of critical information infrastructure, whose national mission includes watching, warning, response and recovery efforts, and the facilitation of collaboration between government entities, the private sector, academia and the international community. Collaboration is necessary to effectively align capabilities and expertise to manage incidents and raise awareness of potential incidents and steps toward remediation. Government has the key role in ensuring coordination among these entities.

Generally, the establishment of a national incident management system requires the following:

1. Establishing a legal framework

2. Setting up a governmental lead institution that is responsible for coordinating and overseeing a national CERT

3. Developing a plan for operation, international collaboration and funding

A legal framework enables the CERT to function effectively by extending existing or enacting appropriate legislation. The legislation can encourage cooperation among stakeholders and reporting of security incidents to the national CERT. The CERT generally operates under the control of a government agency. It is therefore important to establish a lead government agency to coordinate and oversee the operation of a national CERT. Moreover, extensive planning needs to take place before a CERT is developed and implemented. This includes identifying key stakeholders and participants in the development process; developing a strategic plan and vision for how the CERT will be organized, structured, staffed and funded; training the CERT staff; and incorporating mechanisms to evaluate and improve CERT operations.

National CERTs should be established under a legal framework to supervise compliance, collect information on incident and threats to information security, investigate violations of and threats to information security, and publicize information security matters. The main role of a CERT is to provide services and support to prevent and respond to cybersecurity-related issues and serves as a single POC for cybersecurity incident reporting, coordination and communication. The mission of a CERT generally includes analysis, warning, information sharing, vulnerability reduction, mitigation and aiding national recovery efforts for critical information infrastructure. A CERT normally works together with appropriate authorities, but does not direct or control their activities.

44 This sub-section is drawn heavily from: ITU, "ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts".

Specifically, a CERT should perform several functions at the national level including, but not limited to:

- Detecting and identifying anomalous activity
- Analysing cyberthreats and vulnerabilities and disseminating cyberthreat warning information
- Analysing and synthesizing incident and vulnerability information disseminated by others, including vendors and technology experts to provide an assessment for interested stakeholders
- Establishing trusted communication mechanisms and facilitating communication among stakeholders to share information and address cybersecurity issues
- Providing early warning information, including information about mitigating vulnerabilities and potential problems
- Developing mitigation and response strategies and effecting a coordinated response to the incident
- Sharing data and information about the incident and corresponding responses
- Tracking and monitoring information to determine trends and long term remediation strategies
- Publicizing general cybersecurity best practices and guidance for incident response and prevention

5.4.1 Specific Steps for Establishing a National CERT

1. **Establish mechanism(s) within government for coordination among civilian and government agencies**

- A key role for a CERT is to disseminate information, including information about current vulnerabilities and threats, to interested stakeholders. One stakeholder community that must be engaged in response activities is relevant government agencies.
- Effective coordination can take a number of forms, for example: maintaining a website for exchanging information; providing information via mailing lists, including newsletters, trends and analysis reports; and producing publications that include alerts, tips and information about various aspects of cybersecurity including new technologies, vulnerabilities, threats and consequences.

2. **Establish collaborative relationships with the private sector to prepare for, detect, respond to and recover from national cyberincidents**

    - As the private sector in many countries owns much of the critical information infrastructure and ICT assets, government must work with the private sector to achieve its overarching goal of effective incident management.
    - Collaborative relationships with the private sector that are built on trust allow governments to gain insight into the critical infrastructure that is owned and operated by the private sector. Public-private-peoples collaboration can help manage risk associated with cyberthreats, vulnerabilities and consequences and build situational awareness through information sharing, outreach and mutual engagements.

- Encourage the development of sharing practices between the private sector and government that enable sharing of operational information in real time. A few ways to encourage this collaboration may include:

  - Identifying the benefits for both government and the private sector

  - Developing and implementing programmes that ensure the protection of sensitive proprietary data

  - Establishing public-private working groups on cyber-risk management and incident management

  - Sharing incident response/management best practices and training materials

  - Collaboratively defining government and private sector roles and responsibilities for incident management, to put in place consistent, predictable protocols over time

3. **Establish point(s) of contact within government agencies, the private sector and international partners to facilitate consultation, cooperation and information exchange with the CERT**

   - Identifying appropriate points of contact and establishing collaborative working relationships for consultation, cooperation and information exchange are fundamental to a coordinated and effective national and international incident response mechanism. These relationships can promote early warning of potential cyberincidents and exchange of information about trends, threats and responses among incident response entities and other stakeholders.

   - Maintaining up-to-date points of contacts and communication channels with stakeholder communities can provide proactive, timely information exchange about trends and threats and expedite responses. It is important, to the extent possible, to establish contacts based on departmental functions rather than with individuals to ensure that communication channels remain open even when individuals leave an organization. Relationships often begin by establishing trust with particular individuals, but should evolve into more formal, institutional arrangements.

4. **Participate in international cooperative and information sharing activities**

   - Governments should encourage collaboration with organizations, vendors and other appropriate subject matter experts to: (1) advance incident response as a discipline worldwide; (2) promote and support possibilities for CERTs to participate in global and regional conferences and forums, in order to build their capacity; and (3) collaborate on the development of materials for establishing national CERTs and for effectively communicating with the CERT authorities.

5. **Develop tools and procedures for the protection of the cyber-resources of government entities**

   - Effective incident management requires the development and implementation of policies, procedures, methodologies, security controls and tools to protect government cyberassets, systems, networks and functions. For a CERT, these can include standard operating procedures, guidelines for internal and external operations, security policies for coordinating with stakeholders, implementation of secure information networks for CERTs operations, and secure communications. As a focal point for incident response, CERTs should coordinate with each other and help enable collaboration with other

incident response entities. Governments should also provide continual incident response training to new and existing staff.

6. **Develop capability through the CERT for coordination of governmental operations to respond to and recover from large-scale cyberattacks**

    - If there is an incident that rises to the level of national significance, there will be a need for a central POC to coordinate with other governmental entities as with other stakeholder communities, such as the private sector. It is important to develop plans and procedures to ensure that the CERT is prepared to address a possible incident.

7. **Promote responsible disclosure practices to protect operations and the integrity of the cyberinfrastructure**

    - Occasionally, vulnerabilities in ICT products such as hardware and software may be discovered. Decisions on public disclosure should be made on a case by case basis so that vulnerability information is not misused. Vendors should be given ample time in advance of any such disclosure to such vulnerabilities.

5.5 Case Studies

5.5.1 Republic of Korea

Information security promotion systems in the Republic of Korea can be divided into national cybersecurity systems, e-government security systems, critical information infrastructure security systems and private information security systems. With respect to the national cybersecurity system, the National Cyber Security Management Regulation was issued by a presidential directive on 31 January 2005, which regulates cybersecurity organizations such as the National Cyber Security Strategy Council and the NCSC. Meanwhile for e-government security systems, the Act on Promotion of Electronic Administration for e-Government, enacted on 28 February 2001, regulates matters of information protection as well as e-government.

If a cyberincident takes place, NCSC staff is dispatched to the site to investigate its cause and swiftly restore the system. The NCSC staff also examines the security of systems to prevent similar incidents in advance. Furthermore, the security centre has organized a response team alliance dealing with national cyberattacks, and is installing an emergency contact system for affected organizations.

The NCSC takes preventive measures against cyberthreats. It also analyses collected information on IT security, traffic and capacity, using the service networks of numerous organizations, including government high-speed networks. Moreover, NCSC issues color-coded cyberthreat warnings (green, blue, yellow, orange and red). It also distributes various security guidelines and information on worms and viruses, security news, cyberincidents and security technology to the private, public and military sectors.

The KISA under auspices of the KCC operates the KrCERT, which is located in a separate secure specialized area at KISA. The KrCERT derives its mandate from the Act on Promotion of Information & Communication Network Utilization and Information Protection. In article 48-2 of the Report on Infringement Accident, etc., it states that:

1. The KCC shall perform the task falling under each of the following subparagraphs to properly cope with any infringement accident and may, if necessary, get the Security Agency to perform the task, in whole or in part:

- The collection and dissemination of information on infringement accidents;
- The forecast and alert of infringement accidents;
- Emergency measures against infringement accidents; and
- Other measures prescribed by the Presidential Decree to cope with infringement accidents.

2. The person falling under each of the following subparagraphs shall furnish information pertaining to infringement accidents, including the statistics related to infringement accidents by type, the statistics of traffic volume in the relevant information and communication networks and the statistics of uses by connection channel, to the MIC or the Security Agency under the conditions as prescribed by the Ordinance of the MIC:

- The provider of major information and communication services;
- The business operator of agglomerated information and communication facilities; and
- Other person who is prescribed by the Presidential Decree as the operator of the information and communication networks.

Article 48-3 in the Report on Infringement Accident, etc., states that: The person falling under each of the following subparagraphs shall, when any infringement accident occurs or he finds signs of any infringement accident, report without delay the occurrence of such infringement accident or his finding of such signs to the Minister of Information and Communication or the Security Agency. In this case, if any notice is served in accordance with Article 13 (1) of the Act on the Protection of Information and Communications Infrastructure, such notice shall be deemed the report referred to in the former part:

- The provider of information and communication services;
- The business operator of agglomerated information and communication facilities; and
- Other person who is prescribed by the Presidential Decree as the operator of the information and communication networks.

5.5.2 Finland

The Finnish national CERT, CERT-FI[45] is managed by the Finnish Communications Regulatory Authority (FICORA). CERT-FI was established in 2002 under law to supervise compliance, collect information on violations of and threats to information security, investigate violations of and threats to information security and publicize information about security matters. The CERT is a national point of contact for security coordination and incident handling, information security awareness and vulnerability coordination.

The CERT-FI operates under the Network and Security Department in FICORA. This direct linkage with the regulator and the location is advantageous, facilitating communication and coordination of activities with operators and service providers. The CERT-FI is located in a separate secure

45 http://www.cert.fi/en/index.html.

specialized area at FICORA and is a Unix/Linux-based environment recommended for download of malicious code for analysis. The CERT-FI has adopted a bottom-up way of working and uses wiki[46] for internal organization and information sharing. The CERT-FI has dependable and separate Internet connections to allow secure analysis of malware and malicious code plus 3G connections providing redundancy.

The FICORA derives its mandate for from the Act on the Protection of Privacy in Electronic Communications, Chapter 5: Information Security in Communication, Section 31 that states the duties of the regulator are as follows:

- To supervise compliance with the Act
- To collect information on violations of and threats to information security in respect of network services, communication services and value added services, and on significant faults and disruptions in such services
- To investigate violations of and threats to information security in respect of network services, communication services and value-added services, and significant faults and disruptions in such services
- To publicize information security matters

46 For more information on what a wiki is see http://en.wikipedia.org/wiki/Wiki.

Summary

- A national incident management system provides a consistent nationwide framework and approach to enable government at all levels, the private sector and non-governmental organizations to work together to prepare for, prevent, respond to, recover from and mitigate the effects of incidents regardless of the incident's cause, size, location, or complexity.
- The CERT is defined as a service organization responsible for receiving, reviewing and responding to computer security incidents reports and activity and provides the necessary services to handle them and support their constituents to recover from breaches.
- Incident handling flows through three phases: pre-phase, emergency phase and after-phase.
- An incident can be assessed using a classification system based on the "seriousness" of the incident. The system provides four classes of seriousness—Class 1 being of no consequences to Class 4 being very serious.
- To protect the organization assets, the organization should implement three protection mechanisms: preventive mechanism, detection mechanism and reacting mechanism.
- Generally, the establishment of a national incident management system requires: the establishment of a legal framework; setting up of a governmental lead institution that is responsible for coordinating and overseeing a national CERT; and development of a plan for operation, international collaboration and funding.
- Specific steps for establishing a national CERT include:
  - Establishing mechanism(s) within government for coordination among civilian and government agencies
  - Establishing collaborative relationships with the private sector to prepare for, detect, respond to and recover from national cyberincidents
  - Establishing point(s) of contact within government agencies, the private sector and international partners to facilitate consultation, cooperation and information exchange with the CERT
  - Participating in international cooperative and information sharing activities
  - Developing tools and procedures for the protection of the cyber-resources of government entities
  - Developing capability through the CERT for coordination of governmental operations to respond to and recover from large-scale cyberattacks
  - Promoting responsible disclosure practices to protect operations and the integrity of the cyberinfrastructure

This chapter can be used by policymakers to establish incident response policies.

6. THE COMMON CRITERIA FOR INFORMATION SECURITY SOLUTIONS

You will find in this chapter discussions on:

- **An overview of the Common Criteria (CC) and the Common Criteria Recognition Arrangement (CCRA);**
- **The structure of CC (ISO 15408) and certification procedures; and**
- **Trends of certificated solutions.**

6.1 Overview of the CC and the CCRA

To ensure the information security level of the products or the solutions, a third party's evaluation and assurance are required. This is particularly relevant when the security requirements of the products have not been fully implemented and the vulnerabilities of software have not been found at the development stage.

The CC for information security evaluation is based on an international technical standard (ISO/IEC 15408) to validate that information security solutions satisfy a defined set of technical requirements. Targets of CC evaluation are widely ranged from hardware and firmware to software and composited solutions. Vendors can implement or make claims about the security functions of their solutions and development procedures, and testing teams can evaluate the products to determine if they technically follow the claims in the evaluation process.

The objectives of the CC are as follows:

- The CC allows IT users to protect their information assets from cyberincidents more effectively by deploying highly qualified information security solutions.
- The CC can be utilized by IT users as a purchasing guideline for information security solutions.
- The information security industry benefits from the CC in terms of cost minimization, time saving and in the exportation of their products by the mutual recognition of the CC certification.

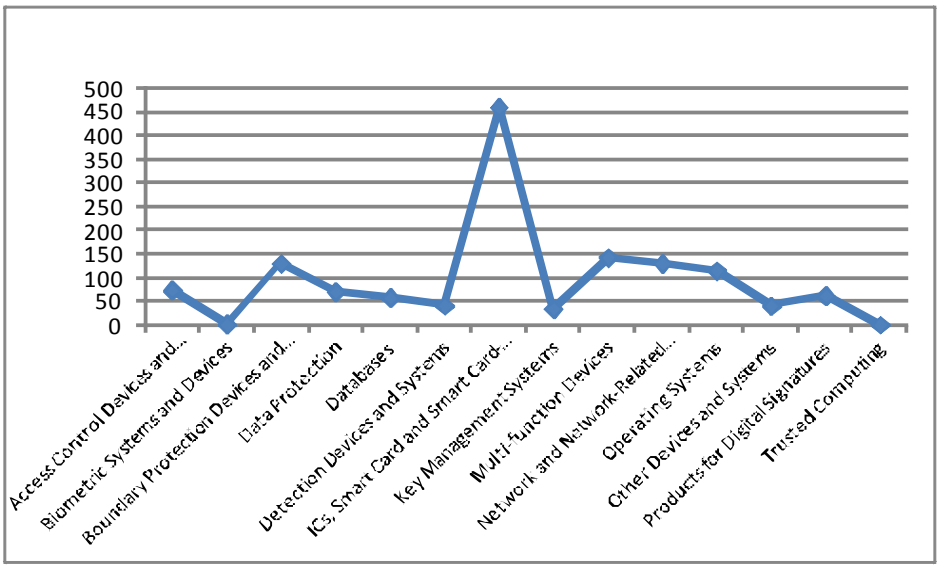
The CCRA is a multinational agreement among countries to recognize the evaluations against the CC standard done by other parties.

To introduce the certification and evaluation systems for trusted information security solutions, the certification and evaluation organizations should be designated under the related laws. In most cases, the certification organizations are governmental agencies, but evaluation organizations sometimes take the form of a public or private company. The roles of the evaluation organization includes: performing evaluation of information security solutions; establishing and managing evaluation procedure rules; and evaluating security assurance level based on the CCRA's technical standards. These roles of the evaluation organization are assigned by the certification organization.

For this, related law or regulation must be established at the government level, and it is important to regulate the relation among the certification organizations, evaluation organizations and vendors. In the case of the Republic of Korea, the regulation for the evaluation and authentication of information security solutions is managed by the MOPAS. Regulations are in place for evaluation and authentication partnership, evaluation procedure, authentication procedure, following up control, and evaluation fee structure.

Figure 10 shows recent trends of certificated solutions within the CCRA. Access control tools such as integrated circuits and smart cards are most active among the recently certificated solutions, and the number of related and new solutions is rising with the convergence of ICTs. In the case of the EU, for example, the range of CC-evaluated solutions will be expended to electronic payment devices, electronic voting devices and taximeters.

Figure 10. Number of certifications registered with the CCRA



Source: http://www.commoncriteriaportal.org.

6.2 Structure of the CC (ISO 15408)

To meet the information security requirement, the CC provides the technical standards of the security performance and reliability. The CC is comprised of three parts. The CC Part 1[47] is an introduction to CC, with general concepts defined and the principles of evaluating the information security systems discussed. It also explains the purpose of the information security systems and the structures for writing the upper level details of the information security systems.

The CC Part 2[48] defines the security functional requirements for the purpose of evaluating IT products. The functional requirements are expressed in classes, families and components. The 11 classes include: security audit, communication, cryptographic support, user data protection, identification and authentication, security management, privacy, protection of the target of evaluation (TOE)[49] security function, resource utilization, TOE access, and trusted path/channels.

The CC Part 3[50] describes the standard evaluation items of the security assurance components. The Evaluation Assurance Level (EAL) is used to evaluate the IT products, and the Composite Assurance Package is used as the certification level for the compounded products with the evaluated and unevaluated IT components. The relevant classes are as follows: Protection

47 Common Criteria, Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 3, Final (July 2009). Available at http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf (accessed on 17 February 2012).

48 Common Criteria, Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1, Revision 3, Final (July 2009). Available at http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3%20-%20marked%20changes.pdf (accessed on 17 February 2012).

49 TOE is the product or system that is the subject of the evaluation. http://en.wikipedia.org/wiki/Common_Criteria.

50 Common Criteria, Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, Revision 3, Final (July 2009). Available at http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3%20-%20marked%20changes.pdf (accessed on 17 February 2012).

Profile[51] evaluation, Security Target[52] evaluation, development, guidance documents, life cycle support, tests, vulnerability assessment and composition.

Table 3. Road map to the CC

	Part 1	Part 2	Part 3
Consumers	Use for background information and for reference purposes. Guidance structure for Protection Profiles	Use for guidance and reference when formulating statements of requirements for a TOE	Use for guidance when determining required levels of assurance
Developers	Use for background information and reference purposes. Use for the development of security specifications for TOEs	Use for reference when interpreting statements of functional requirements and formulating functional specifications for TOEs	Use for reference when interpreting statements of functional requirements
Evaluators	Use for reference purposes and for guidance in the structure for Protection Profiles and Security Targets	Use for reference when interpreting statements of assurance requirements and determining assurance approaches of TOEs	Use for reference when interpreting statements of assurance requirements

Source: Common Criteria, Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 3, Final (July 2009). Available at http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf (accessed on 17 February 2012).

The EAL is the numerical rating describing the depth and rigour of an evaluation. Each EAL corresponds to a package of security assurance requirements[53] that covers the complete development of a product, with a given level of strictness. Common Criteria lists seven levels, with EAL 1 being the most basic (and therefore cheapest to implement and evaluate) and EAL 7 being the most stringent (and most expensive). Higher EALs do not necessarily imply "better

51 A Protection Profile is a document typically created by a user or user community that identifies security requirements for a class of security devices (e.g., smart cards used to provide digital signatures, or network firewalls) relevant to that user for a particular purpose. Product vendors can choose to implement products that comply with one or more Protection Profiles, and have their products evaluated against those Protection Profiles. In such a case, a Protection Profile may serve as a template for the product's Security Target (defined below), or the authors of the Security Target will at least ensure that all requirements in relevant Protection Profiles also appear in the target's Security Target document. Customers looking for particular types of products can focus on those certified against the Protection Profile that meets their requirements. http://en.wikipedia.org/wiki/Common_Criteria.

52 A Security Target is a document that identifies the security properties of the TOE. It may refer to one or more Protection Profiles. This allows vendors to tailor the evaluation to accurately match the intended capabilities of their product. This means that a network firewall does not have to meet the same functional requirements as a database management system, and that different firewalls may in fact be evaluated against completely different lists of requirements. The Security Target is usually published so that potential customers may determine the specific security features that have been certified by the evaluation. http://en.wikipedia.org/wiki/Common_Criteria.

53 Security Assurance Requirements are descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality. For example, an evaluation may require that all source code is kept in a change management system, or that full functional testing is performed. The Common Criteria provides a catalogue of these, and the requirements may vary from one evaluation to the next. The requirements for particular targets or types of products are documented in the Security Target and Protection Profile, respectively. http://en.wikipedia.org/wiki/Common_Criteria.

security", they only mean that the claimed security assurance of the TOE has been more extensively verified.[54]

6.3 Certification Procedure of the CC

The organizational structure for evaluating and certifying security products includes the policy authority, certification organizations and evaluation organizations. The policy authority establishes the direction, standards, guidelines and notifications related to certification and evaluation. The certification organization is responsible for the management of the evaluation organization, that is, approval of evaluator, assignation of evaluation organizations, establishment of certification regulations and issuance of the certificates. The evaluation organization evaluates submitted information security products.

Based on a best practice from the Republic of Korea, the certification procedure is composed of four stages: preparation, evaluation, certification and follow-up.[55] In the preparation stage, the company requiring certification applies for evaluation and engages in a contract with the evaluation organization. The evaluation organization performs the evaluation, including verification of design error, testing of security functions and verification of vulnerability, based on the products submitted. As the evaluation organization completes the evaluation, the certification organization reviews the report and issues a certificate. For the certified product of which configuration is changed, the company applies for follow-up evaluation in order to maintain the assurance period of the product.

6.3.1 Preparation Stage

In the preparation stage, the application and contract for evaluation are made. The company requiring CC certification consults with the evaluation organization on the preparation for application.

The applicant for evaluation submits the product based on the information acquired from the consultation. The evaluation organization reviews the Protection Profile or Security Target products, and advises the applicants on supplementation required for proper evaluation.

The applicant prepares the application for evaluation, and submits the application with the product and documents. In receiving the application for evaluation, the evaluation organization makes a contract with the applicant and notifies the certification organization of the details of the application.

6.3.2 Evaluation Stage

The evaluation stage is the key part of the evaluation procedure. It consists of organization of an evaluation team after the contract is made, evaluation of the product submitted and preparation of the evaluation report. The evaluation organization organizes an evaluation team consisting of the evaluation team leader and the evaluators.

54 Adapted from Wikipedia, "Common Criteria". Available at http://en.wikipedia.org/wiki/Common_Criteria.

55 KISA, IT Security Evaluation & Certification Guide with Common Criteria (ISO 15408), April 2009.

The applicant holds a presentation on the product in order to help the evaluation organization understand the product submitted. The presentation includes explanation on the product and demonstration of the functions. After the presentation, the evaluation organization prepares and submits the evaluation plan to the certification organization to acquire approval.

The evaluation team evaluates the product submitted, and in the course of the evaluation, visits the applicant and performs a security evaluation on the development environment. Upon receiving a request from the evaluation organization to resolve any issues or problems found from the evaluation of the product and/or the company, the applicant must address the issues or problems during the evaluation stage, and submit the results to the evaluation organization.

At the end of the evaluation stage, the evaluation organization prepares and submits the evaluation report to the certification organization. If the applicant fails to resolve the issues or problems identified by the evaluation team without reason, or if it is considered difficult to continue evaluation due to a reason attributable to the applicant, the evaluation process is stopped for a certain period or the evaluation contract is cancelled.

6.3.3 Certification Stage

In the certification stage, the certification committee deliberates the application, and issues the certificate and the certification result statement. When the evaluation organization submits the evaluation report, the certification organization assembles the certification committee to review the validity and fairness of the evaluation result.

The certification committee reviews and analyses the evaluation report, verifies if the evaluation has been performed in compliance with the requirements of the CC, the common evaluation methodology and the evaluation systems of other countries, judges suitability, and prepares the summary of the evaluation result.

If the application successfully passes the verification of the certification committee, the certification organization issues the certificate and the certification result statement to the applicant, and records the certified product in the certified product register. The evaluation organization returns the source program of the certified product to the applicant, and keeps other documents for the validity period of the certificate.

6.3.4 Follow-Up Stage

If there is a functional change in the certified product, the applicant must prepare the security impact analysis report, and apply for maintenance of the validity of certification. The certification organization reviews the change, and determines whether to approve the change or to re-evaluate the product. The product can maintain validity of certification only when the functional change is approved.

6.4 Case Study from the Republic of Korea

The Republic of Korea developed the first independent evaluation criteria in February 1998. The evaluation products were firewall (1998); intrusion protection system (2000); virtual private network (2002); and secure operating system, fingerprint verification system and smart card (2003). Since 2002, both Korean evaluation criteria and the CC are being used. In 2005, the

scope of the evaluation products expanded to all the information security products, and became a Composite Assurance Package of CCRA in May 2006.

The CC policy authority in the Republic of Korea is MOPAS, and the certification organization is the Information Technology Security Certification. As of 2011, evaluation organizations include KISA, the Korea Security Evaluation Laboratory, the Korea System Assurance, the Korea Testing Laboratory and the Telecommunications Technology Association. For the supply of security products to public organizations in the Korean market, all the security products must have CC certification level of EAL 2 or higher.

Summary

- The CC for information security evaluation is based on an international technical standard (ISO/IEC 15408) to validate that information security solutions satisfy a defined set of technical requirements. It focuses on the evaluation of information security levels rather than development of requirements. But most requirements of developers are accepted in the evaluation process by the evaluators.

- The CC is comprised of three parts. CC Part 1 is an introduction to CC, with general concepts defined and the principles of evaluating the information security systems discussed. Part 2 defines the security functional requirements for the purpose of evaluating IT products. Part 3 describes the standard items for evaluation of the security assurance components.

- The certification procedures consist of four stages: preparation, evaluation, certification and follow-up. In the preparation stage, the company requiring certification applies for evaluation and engages in a contract with the evaluation organization. In the evaluation stage, evaluators conduct the evaluation on the products submitted, including verification of design error, testing of security functions and verification of vulnerability.

This chapter can be used by policymakers to put in place certification procedures based on the CC.

7. PERSONAL INFORMATION PROTECTION

You will find in this chapter discussions on:

- **An overview of personal information protection;**
- **Issues in personal information protection**
- **Different measures for personal information protection—legal and regulatory measures, technical measures and cultural measures; and**
- **Legal trends in the OECD member countries.**

7.1 Overview of Personal Information Protection

Personal information can be defined as information that can be used to uniquely identify, contact or locate a single person or can be used with other sources to uniquely identify a single individual.[56] A person can be identified by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

Personal information can be classified in many different ways, including biological information, sociological information, institutional information and electronic personal information. The classification of personal information helps to determine various procedures for personal information handling, for example, based on the sensitivity of the personal information. The different classes of personal information include the following:[57]

- General information, e.g., name, driver's license number, address, telephone number, birth date, birth place, sex, nationality
- Family information, e.g., names, birth place, birth date, occupations of family members
- Education and training information, e.g., schools, school grades, certificates and licenses, completed training programmes, awards
- Property information, e.g., houses, land, buildings, cars
- Income information, e.g., annual salary, interest income, business income
- Credit information, e.g., loans, collateral, credit cards, payables
- Employment information, e.g., employer, company address, evaluation record, attendance, awards, work attitude
- Legal information, e.g., criminal record, traffic record, bankruptcy and collateral, imprisonment, divorce, tax returns
- Medical information, e.g., physical record, disability, blood type, IQ, drug test
- Organization information, e.g., union membership, religion organization membership, political party membership, club membership
- Communication information, e.g., e-mails, call history, log files, cookies
- Location information, e.g., individual's location information by GPS or mobile phone
- Physical information, e.g., finger prints, iris, DNA, height, chest size
- Habit and hobby information, e.g., hobbies, smoking, alcohol consumption

Although the concept of personal information is old, it has become much more important as ICTs and the Internet have made it easier to collect personal information, leading to a profitable market in collecting and reselling personal information. Personal information can also be exploited by criminals to stalk or steal the identity of a person, or to plan a person's murder or robbery, among other crimes. As a response to these threats, many website privacy policies specifically address the collection of personal information, and lawmakers have enacted a series of legislation to limit the distribution and accessibility of personal information.[58]

56 Wikipedia, "Personally identifiable information". Available at http://en.wikipedia.org/wiki/Personal_Information (accessed on 18 February 2012).

57 KISA, Data protection activities in advanced countries (June 2009).

58 Wikipedia, "Personally identifiable information".

The OECD has developed a number of guidelines related to personal information protection. Two important guidelines stand out. It includes the 1980 “OECD Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data”, also known as the OECD Fair Information Practices. In 2002, “Privacy Online: OECD Guidance on Policy and Practice” was published. In this guidance, OECD advised to observe the following eight principles for personal information protection: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness principle, individual participation, and accountability.

As the OECD’s eight principles for personal information protection are the minimum standards that are advised to its member countries, they became the model of many countries’ personal information protection related laws, regulations and guidelines.

7.2 Global Issues in Personal Information Protection

Personal information is present in many forms as the type of ICT equipment become more diversified and advanced. An individual’s image information and location information can be captured through closed circuit television, call history and location information can be retrieved from mobile devices, and the use of biometric authentication can provides physical information.

Therefore, either voluntarily or involuntarily, most individuals have to provide their own information in order to use the services provided by public institutions and corporations. As various corporate marketing also makes use of personal information, personal information’s monetary value increases, resulting in cybercriminal acts such as the illegal transaction of personal information and infringement of privacy.

Moreover, personal information invasion has increased together with the growth of online business transactions. For example, when spam mail is sent, the sender manipulates the information or set up as send-only so that the recipient cannot reject the mail although he/she checks for rejection. In adult advertising mail, one may have to go through the process of confirming that you are an adult by providing the resident registration number in order to reject the mail.

Leakage patterns of personal information are as follows:

- Exposure from open websites: The collection of personal information from open websites occurs frequently. This could be done manually by surfing the websites, or automated with the use of software.

- Data leakage by insiders: The use of personalized online services often begins with entering a username and password. For this, service providers store massive personal information, so there is a risk of these being misused or abused. Therefore, encoding technology is necessary to prevent personal information from leakage, misuse or abuse by insiders.

- Sniffing of online transactions: Online transactions made through online banking or credit cards can be hacked. It is possible for hackers to intercept online banking login credentials and credit card information to log in to the victim’s online banking account or purchase items with the victim’s credit card.

- Illegal use of cookies in personal computers: A cookie is a small text file that a Web server stores on a user’s hard drive when the user visits certain websites. A cookie can contain information used for authentication, identification of a user session, user preferences, shopping cart contents, or anything else that can be accomplished through storing text data. When a user revisits that website, the information in the cookie is sent back to the

site so that the site can tailor what it presents to the user, for example, the tastes in music or shopping habits, and/or name of user on the welcome page. Cookies can be used by spyware to track user's browsing activities. Cookies can also be stolen by hackers to gain access to a victim's Web account.

- Dealing with personal information: Customer's personal information is transacted openly when relevant laws are incomplete or its punishment is not rigid enough. The trend now is towards harsher punishments for illegally obtaining personal information and privacy infringement.

7.3 Personal Information Protection Policy

Governments have developed various policies to prevent illegal hacking, internal data leakage and misuse or abuse of personal information. These various policies for personal information protection include legal and regulatory measures, technical measures and cultural measures.

7.3.1 Legal and Regulatory Measures

As the proper handling of personal information by public and private sectors become critical, the legal basis to protect citizen's personal information needs to be prepared and enforced. Furthermore, it is important to establish an independent personal information protection supervisory authority in order to carry out overall duties for protection of citizens' privacy and rights, and prevent in advance any possible conflict.

The EU and OECD have proposed several guidelines to protect personal information systematically and organizationally, and international standard organization such as the International Organization for Standardization (ISO) also provides detailed guidelines.

A privacy impact assessment is a systematic process of investigating, analysing and evaluating new information systems that utilizes personal information or the modification of such existing information systems. It assesses the impact of these systems on individuals' or a nation's privacy. It is not simply a system of evaluation but includes analysis of the serious effects on privacy when new systems are introduced or when changes are made to systems. A privacy impact assessment is performed on new and modified systems that hold and manage a large quantity of personal information, such as an e-government service.

7.3.2 Technical Measures

In order to block personal information leakage technically, information security technologies such as database encryption, data leakage protection and access control technology are needed. These technologies protect personal information from activities such as illegal information use, leakage, modification and deletion.

The following technologies need to be developed:

- A technology that limits a business person from information collection other than necessary information

- A technology that can clarify a business person's exposure to personal information protection policy, information process procedure and use purpose

- A technology that offers information subjects an option to decide about his/her own information by him/herself
- A technology that limits a third person's use of information for purposes other than intended
- A technology that offers the information subject approving authority when information is provided to a third person
- A technology that maintains security for safe and reliable information processing procedures for information misuse and abuse

As most Internet services users utilize Web services, developing technologies that can strengthen Web server's weak security function is required to protect personal information that is maintained, recorded and distributed on the Web.

Technical solutions for protecting personal information online include: P3P,[59] privacy policy generator, cookies management program, advertisement blocking program, encoding product, Web surfing anonymity product and third person proxy service.

7.3.3 Cultural Measures

Self-Regulation of Personal Information Handler

In order to effectively protect personal information, the qualification and quality of a person in charge of personal information protection are important. Related to qualifications, he/she needs to have a comprehensive understanding of personal information protection related rules. And related to quality, he/she has to realize that personal information is not the object of business transactions but a shortcut in customer protection.

At the same time, it is crucial that the personal information handler follows information protection management guidelines.

- The personal information handler has to observe the set of guidelines on the purpose, procedures and provisions of personal information collection.
- When the personal information handler needs to use other's personal information, he/she has to obtain the approval from the personal information subject, use the personal information within the range of the collection purpose, and use caution in managing sensitive information like physical information.
- When personal information is unnecessary, the holding period is expired and the information subject agrees, the personal information handler has to delete or reformat personal information to prevent leakage.

Most legal regulations related to personal information protection are ex post facto regulations that impose sanctions, and their application objects are often limited to certain personal information handlers. However, with the rapid advancement of ICTs and the increasing complexity of personal information protection, self-regulation by industries such as through trade association and social regulation is crucial.

59 The Platform for Privacy Preferences Project, or P3P, is a protocol allowing websites to declare their intended use of information they collect about browsing users. Designed to give users more control of their personal information when browsing, P3P was developed by the World Wide Web Consortium and officially recommended on 16 April 2002. Wikipedia, "P3P". Available at http://en.wikipedia.org/wiki/P3P (accessed on 18 February 2012).

Awareness and Education

Complementing top-down enforcement, there is an urgent need to promote public education and raise awareness on the importance of personal information protection among government officials, businesses and the general public. A forum for personal information handlers to share knowledge and experience on the different measures available for protecting personal information would be useful.

Children's Personal Information Protection

The Internet has become a major source for marketing, sales and distribution of products and services; and a growing segment of users of these services are children. Studies revealing that children are less able to understand the potential effects of disclosing their personal information, and that huge amounts of private information on children have been released into the market, have prompted the need for regulation.[60]

In the USA, the Children's Online Privacy Protection Act of 1998 became effective on 21 April 2000. The Act specifically protects the privacy of children under the age of 13 by requesting parental consent for the collection or use of any personal information of the users. In the Republic of Korea, a regulation states that parental consent is needed for children younger than the age of 14. In Japan, parental consent is needed for children between the age of 12 and 15.

7.4 The Legal Trends of OECD Member Countries[61]

7.4.1 Republic of Korea

In the Republic of Korea, personal information has been protected under different laws, with separate laws for the public and private sectors. To raise the level of protection in private areas where there had been no applicable laws, the Personal Information Protection Act was established. The Personal Information Protection Act passed the National Assembly on 29 March 2011, and took effect on 30 September 2011. The main purpose of this act is to: (1) eliminate "blind spots" that exits because of the absence of laws regulating offline businesses and non-profit organizations; (2) meet the needs for the adoption of global standards related to the Privacy Protection Law; and (3) protect the rights of individuals by strengthening the right to informational self-determination and legal action against rights violations against individuals.

For individual laws and relevant laws, there are the Protection of Communications Secrets Act (1993), the Credit Information Protection and Usage Act (1995), the Electronic Business Transaction Fundamental Law (1999, 2005), and the Information Network Usage and Protection Act (2000).

The supervisory institution for information protection in the Republic of Korea is the Personal Information Protection Committee that is affiliated to the President. The committee deliberates and votes on personal information protection related policies, and the MOPAS handles and coordinates personal information protection implementation.

60 Electronic Privacy Information Center, "Children's Online Privacy Protection Act (COPPA)". Available at http://epic.org/privacy/kids (accessed on 18 February 2012).

61 This section is drawn from KISA, Data protection activities in advanced countries (June 2009).

7.4.2 Australia

Australia adopted the OECD privacy principles in 1980 and enforced privacy guidelines. The Privacy Act 1988 stipulates a number of privacy rights known as the Information Privacy Principles. These principles apply to the Australian government and Australian Capital Territory (ACT) agencies or private sector organizations contracted to these governments. The principles govern when and how personal information can be collected by these government agencies.[62]

The Privacy Act was amended in 2000 to cover the private sector. Schedule 3 of the Privacy Act sets out a significantly different set of privacy principles (the National Privacy Principles) that apply to private sector organizations (including not-for-profit organizations) with a turnover exceeding AUD 3 million, other than health service providers or traders in personal information. These principles extend to the transfer of personal information out of Australia.[63]

There are a number of other laws related to personal information protection and privacy including the Telecommunications Act 1997,[64] Spam Act 2003[65] and Workplace Video Surveillance Act 1998.[66]

Australia's information protection supervisory institution is the Office of the Privacy Commissioner. Federal institutions report annually to the Federal Privacy Commissioner about personal information's character, owning purpose, classification, holding period and the process for individuals to access information.

7.4.3 Canada

The Personal Information Protection and Electronic Document Act (enacted in 2001)[67] is the comprehensive information protection and privacy law of Canada. It governs how private sector organizations collect, use and disclose personal information in the course of commercial business. In addition, the Act contains various provisions to facilitate the use of electronic documents. The act aims to promote consumer trust in electronic commerce. It is also intended to reassure the EU that the Canadian privacy law was adequate to protect the personal information of European citizens.[68]

The implementation of the Act occurred in three stages. Starting in 2001, the law applied to federally regulated industries (such as airlines, banking and broadcasting). In 2002 the law was expanded to include the health sector. Finally in 2004, any organization that collects personal information in the course of commercial activity was covered by the Act, except in provinces that have "substantially similar" privacy laws.[69]

Two other related acts in Canada include the Access to Information Act (1985) and the Privacy Act (1985). The Access to Information Act gives Canadian citizens the right to access information in federal government records. The Privacy Act provides citizens with the right to access personal information held by the government and protection of that information against unauthorized use and disclosure. The President of the Treasury Board is the Minister responsible for government-wide administration of the legislation, and the supervisory institution is the Office of the Privacy Commissioner established at federal and state governments.[70]

62 Wikipedia, "Privacy Act 1988". Available at http://en.wikipedia.org/wiki/Privacy_Act_1988 (accessed on 18 February 2012).

63 Ibid.

64 http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/.

65 http://www.efa.org.au/Issues/Privacy/spam.html.

66 http://www.austlii.edu.au/au/legis/nsw/repealed_act/wvsa1998295/.

67 http://laws-lois.justice.gc.ca/eng/acts/P-8.6/.

68 Wikipedia, "Personal Information Protection and Electronic Documents Act". Available at http://en.wikipedia.org/wiki/Personal_Information_Protection_and_Electronic_Documents_Act (accessed on 18 February 2012).

69 Ibid.

70 Treasury Board of Canada Secretariat "Access to Information and Privacy". Available at http://www.tbs-sct.gc.ca/atip-aiprp/index-eng.asp (accessed on 18 February 2012).

7.4.4 EU

The EU has comprehensive laws on personal information protection and privacy. An important component is the EU Data Protection Directive (officially known as Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data), which regulates the processing of personal data within the EU. The EU directive was adopted in 1995 and enforced since 1998.

The EU Directive encompasses all key elements from article 8 of the European Convention on Human Rights, which states its intention to respect the rights of privacy in personal and family life, as well as in the home and in personal correspondence. The Directive is based on the 1980 OECD "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data". The main contents of the EU Directive are as follows:

- Personal information should be processed fairly and only authorized persons have a right to access it, including the subjects whose information is being collected.
- Personal information collected should be used only for stated purpose(s) and for no other purposes.
- The purpose of personal information collection and processing should be clear and legitimate, and personal information must be up-to-date.
- Personal information may be processed only if the subjects whose information is being collected have unambiguously given their consent.
- Once collected, personal data should be kept safe and secure from potential abuse, theft or loss.
- An independent and internally or externally controlling institution should be appointed to identify and apply information processing principles and ensure that the process does not affect the subjects' rights or freedom.

The EU established the European Network and Information Security Agency in March 2004 to address information network security problems including personal information protection. The agency developed technology standard and risk assessment methodology, and shared standard the outcomes with member countries.

7.4.5 Japan

Japan's Personal Information Protection Act[71] has been enforced since 2005, and the local governments protect personal information through ordinances. The Act applies to government or private entities that collect, handle and use personal information on 5,000 or more individuals. The law states a set of obligations for companies handling personal information. Companies must designate a manager called a corporate privacy officer and other staff to be responsible for meeting the provisions, and the law also sets fines of up to JPY 300,000 (USD 3,800) or jail sentences up to six months for the manager or data handlers who are found to have not complied.

The Act follows European personal information protection laws in that it adheres to international standards and uses the government sector for regulation. Yet, Japan also emphasizes self-regulation by the business community and avoids excessive regulation.

71 http://www.cs-trans.biz/Personal_Information1.htm.

Other relevant laws include the Public Administration's Personal Information Protection Law, the Independent Administration and Personal Information Protection Law, the Public Information and Personal Information Committee Establishment Law and the Information Security Law.

However, there is no supervisory institution overseeing personal information protection. Instead, the competent minister who governs the sector where personal information handlers conduct their business is given direct supervisory responsibility for personal information protection, which is a unique characteristic of Japan.

7.4.6 United Kingdom

The Data Protection Act 1998 is the main piece of legislation that governs the protection of personal information in the UK. The 1998 Act replaced and consolidated earlier legislation such as the Data Protection Act 1984 and the Access to Personal Files Act 1987. At the same time it aimed to implement the European Data Protection Directive. The Data Protection Act 1998 creates rights for those who have their data stored, and responsibilities for those who store and process personal information.

For individual laws that complement the Data Protection Act, the Consumer Credit Act 1974[72] and the Privacy and Electronic Communications Regulations (2003)[73] are being enforced. These two laws also have a complementary relationship. The supervisory institution is the Office of Information Commissioner.

7.4.7 United States of America

The USA relies on a combination of legislation, regulation and self-regulation, rather than governmental regulation alone in the protection of personal information and privacy. For example, former US President Bill Clinton and former Vice-President Al Gore recommended in their "Framework for Global Electronic Commerce" that the private sector should lead, and companies should implement self-regulation in reaction to issues brought on by Internet technology.[74]

In the USA, there is no comprehensive law comparable to the EU Data Protection Directive. Rather, personal information protection is incorporated in individual laws. The Privacy Act of 1974, for instance, is relevant only to government institutions. Moreover, there is no specialized institution that supervises personal information protection. The Federal Trade Commission handles personal information protection problems only as part of consumer protection.

For US companies doing business in EU countries and who are moving data across their borders will need to comply with the EU Data Protection Directive. To help bridge the differences between the way the US government approaches privacy issues and the EU Directive, the US Department of Commerce consulted with the European Commission and developed the Safe Harbor Privacy Principles. Certifying a US organization to the Safe Harbor requirements will assure the EU entities that the organization provides "adequate" privacy protection as required by the EU Directive.

The enforcement of the California Data Breach Notification Law in 2003 made it mandatory for holders of data to notify consumers whose personal data has been breached. Since then, security breach notification laws have been enacted in most US states.

72 http://www.legislation.gov.uk/ukpga/1974/39/contents.

73 http://www.york.ac.uk/recordsmanagement/dpa/privacyregs.htm.

74 Wikipedia, "Data Protection Directive". Available at http://en.wikipedia.org/wiki/Data_Protection_Directive (accessed on 18 February 2012).

Laws that include protection of personal information in the USA include the following:

- Fair Credit Reporting Act (enacted in 1970)[75]
- Cable Communication Policy Act (enacted in 1984)[76]
- Electronic Communication Privacy Act (enacted in 1984)[77]
- Video Privacy Protection Act (enacted in 1988)[78]
- Health Insurance Portability and Accountability Act (enacted in 1996)[79]
- Right to Financial Privacy Act (enacted in 1999)[80]
- Children's Online Privacy Protection Act (enacted in 1998, enforced in 2000)[81]

Summary

- Although the concept of personal information is old, it has become much more important as ICTs and the Internet have made it easier to collect personal information, leading to a profitable market in collecting and reselling personal information. Personal information can also be exploited by criminals to stalk or steal the identity of a person, or to plan a person's murder or robbery, among other crimes.
- As the proper handling of personal information by public and private sectors become critical, the legal basis to protect citizen's personal information needs to be prepared and enforced. Furthermore, it is important to establish an independent personal information protection supervisory authority in order to carry out overall duties for protection of citizens' privacy and rights.
- The OECD has developed a number of guidelines on personal information protection. OECD's eight principles for personal information protection are the minimum standards that are recommended to its member countries, and they have been widely used in the enactment of personal information protection laws.
- Governments have developed various policies to prevent illegal hacking, internal data leakage and misuse or abuse of personal information. These various policies for personal information protection include legal and regulatory measures, technical measures and cultural measures.

This chapter can be used by policymakers when they address issues of personal information protection and privacy in their countries.

75 http://epic.org/privacy/fcra/.
76 http://en.wikisource.org/wiki/Cable_Communications_Policy_Act_of_1984#SEC._3._JURISDICTION.
77 http://www.answers.com/topic/electronic-communications-privacy-act.
78 http://epic.org/privacy/vppa.
79 http://www.hhs.gov/ocr/privacy/.
80 http://epic.org/privacy/rfpa.
81 http://epic.org/privacy/kids/.

8. CYBERCRIME LAW AND LEGISLATION

You will find in this chapter discussions on:

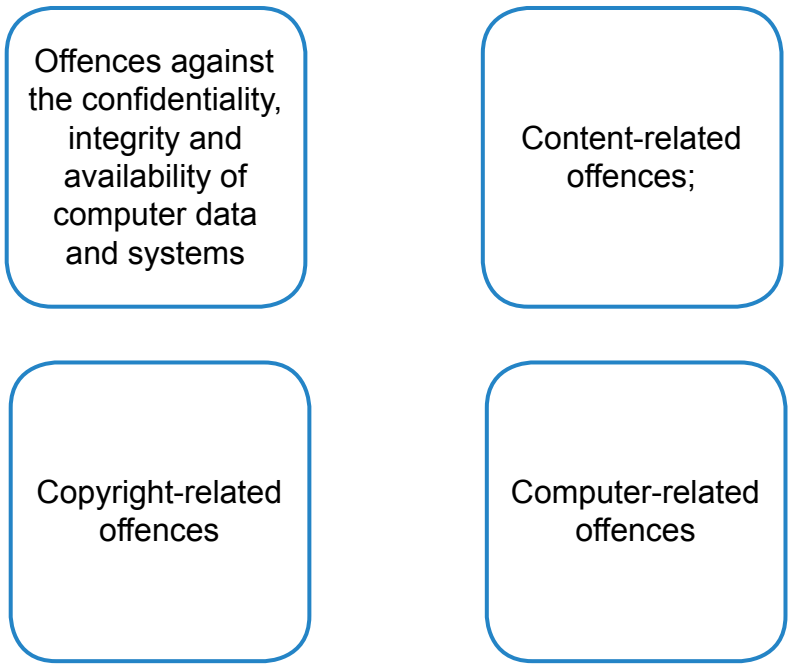
- **An overview of cybercrime;**
- **A classification of cybercrime;**
- **Steps for establishing cybercrime law and legislation; and**
- **Case Studies from the EU and the Republic of Korea.**

8.1 Overview of Cybercrime[82]

Cybercrime is known by a number of different names, such as computer crime, e-crime or electronic crime. All of these crimes are ones where computers or networks are used or attacked. These electronic crimes are being used to steal identities and huge sums of money. Many traditional crimes such as theft, blackmail, forgery, embezzlement and fraud today are all conducted on the Internet. The term "cybercrime" is used to cover a wide variety of criminal conduct. As recognized crimes include a broad range of different offences, it is difficult to develop a classification system for cybercrime. One approach can be found in the Budapest EU Convention on Cybercrime as described in figure 11, which distinguishes between four different types of offences:

1. Offences against the confidentiality, integrity and availability of computer data and systems
2. Content-related offences
3. Copyright-related offences
4. Computer-related offences

Figure 11. Classification of cybercrime



The first three categories focus on the object of legal protection, and the fourth category of "computer-related offences" focuses on the method used to commit the crime. Inconsistencies may lead to some overlap between the classification (refer to Annex).

82 This sub-section is drawn from Marco Gercke, Understanding Cybercrime: A Guide for Developing Countries, ITU Telecommunication Development Sector, 2nd Edition, Draft, March 2011. Available at http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html (accessed 10 January 2012).

8.2 Procedure for Establishing Cybercrime Laws/Regulations[83]

It is important to enact and enforce a comprehensive set of laws relating to cybersecurity and cybercrime consistent with, among others, the provisions of the Convention on Cybercrime (2001). Specific steps to establish cybercrime laws and regulations are as follows:

- **Assess the current legal authorities for adequacy.** A country should review its existing criminal code, including relevant procedures, to determine if it is adequate to address current (and future) problems. Suggested steps are to:
  - Develop, as appropriate, the necessary relevant legislation, noting in particular regional initiatives. Such law should address among other issues, damaging or destroying computer data, procedural mechanisms supporting investigations, and the ability to trace the source of e-mail messages, etc. It should also include possible international legal cooperation, e.g., in procuring evidence.
  - Consider whether its laws rely on outdated technological expectations. For example, a law may discuss the tracing of voice transmissions only. Such a law may need to be changed to cover transmissions of data as well.
  - Have the country's cybercrime law evaluated by all relevant government authorities and legislative bodies that might have an interest in it, even if they have nothing to do with criminal justice, so that no useful idea is missed. An ICT official might notice, for example, that the cybercrime law is inadequate to reach a new technology that is coming into increasing use but is not yet widely known to legal drafters in that country.
  - Have the country's existing criminal law evaluated by some or all of the following: the local private sector, any local affiliate of the international private sector, local non-governmental organizations, academics and recognized experts or groups of citizens.
  - Seek advice on such issues from other countries.
- **Draft and adopt substantive, procedural and mutual assistance laws and policies to address cybercrime.** Suggested steps are to:
  - Participate actively in developing, as appropriate, the necessary legislation, noting in particular regional initiatives, including but not limited to, the Council of Europe Convention on Cybercrime. A country's draft cybercrime law should be evaluated by all government authorities and legislative bodies. Such a draft should also be publicly available for comment in order to address any possible technologies, infractions or other relevant issues that were not originally covered.
  - Engage in regional and international collaboration in order to combat cybercrime and strengthen cybersecurity, and develop mechanisms for enhancing cooperation in cybersecurity.
  - In cybercrime statutes, address not merely classic cybercrimes, such as computer crimes and computer intrusions, but also protect electronic evidence on networks regarding other crimes.
  - Ensure that data protection laws written for civil and commercial life are not extended or interpreted to impede inappropriately the flow of criminal evidence between countries.

83 This sub-section is drawn from ITU, "ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts".

- For countries that decide to hire consultants to do the drafting, consider their qualifications and supervise their work throughout the process. Persons who have not been trained specifically under the law of a country may not adequately integrate all the necessary provisions, especially procedural and mutual legal assistance sections. Moreover, persons who do not have prosecutorial experience are unlikely to adequately consider the practicalities of proving a case. Some consultants are qualified to assist in drafting e-commerce laws but not criminal laws.

- Consult other countries for suggestions beyond what is contained in the convention. For example, countries may require Internet service providers to retain some of the data transiting their systems for some period, often six months; they may require computer incidents of a certain significance to be reported to government authorities; or they may require proper identification before a person uses a cybercafé.

- If time permits, seek comments on the draft cybercrime law (or amendments) from other countries and multilateral organizations. Such comments can be obtained privately and, as noted above, it is helpful to obtain the viewpoints of several countries based on their experience.

- At the earliest possible stage (consistent with national procedures), seek comments also from experts in the subject matter.

- **Establish or identify national cybercrime units.** Suggested steps are to:

  - Regardless of the level of development, have at least a basic cybercrime investigation capacity.

  - Select or train a cybercrime investigative unit that will have competence for national cybercrime investigations. Sometimes it will be obvious which law enforcement service or services this should be. Sometimes competing law enforcement agencies will disagree over the selection and senior authorities will have to make a difficult decision. Even if it appears that the country does not currently have anyone with the necessary skills, it is normally true that there is a law enforcement officer somewhere who is interested in electronic technology and is ambitious to learn more and go further with the field.

  - Support cybercrime investigative units, even if they consist of only a limited number of investigators. They require relatively up-to-date equipment, reasonably reliable network connections and continuing training. Such support may come from the government of the country, from international organizations or other countries, and from private sector donations.

  - Where possible, have at least basic computer forensic capacity in the cybercrime investigative unit. Such capacity will require software tools and additional training. If forensic capacity is considered impossible to achieve, countries should accept beforehand that crucial evidence, even in crucial cases, may be lost. In some circumstances, forensic assistance for specific cases may be available from other countries. In addition, training in cyberforensics may be available, both from other countries and from relevant organizations. For example, the CERT Coordination Center of Carnegie-Mellon University in the USA offers some cyberforensics training for free or at very low prices online or by CD-ROM.

- Once a cybercrime unit is set up, publicize its existence and capabilities to other law enforcement services and to prosecutors in the country. It is pointless having a cybercrime unit in the capital if a regional law enforcement force is investigating a terrible crime that involves electronic evidence but does not know that there is a cybercrime unit that could search the target's computer or offer other help. Unfortunately, it is very common worldwide that a country's law enforcement establishment is unaware that the country possesses a cybercrime unit.

- Foster relationships between the cybercrime units and the international partners to the greatest extent possible. At initial stages, advice about setting up the unit is available from other countries and from international law enforcement organizations. At later stages, training of many types and even equipment and software are available from other countries, from international law enforcement organizations, from relevant multilateral organizations, and from the private sector. Such contacts will also be valuable for another reason: in a world that will become more and more networked, it is critical to be able to request assistance from foreign law enforcement.

- Ensure that every relevant and interested sector, including non-governmental organizations, CERTs, private sector entities and academia are aware of the unit's existence and capabilities, can collaborate with it, and understand how to report possible cybercrime.

• **Develop cooperative relationships with other elements of the national cybersecurity infrastructure and the private sector.** Cooperative relationships among government authorities, other elements of the national cybersecurity infrastructure and the private sector are important for several reasons:

  - To exchange information between these groups (e.g., to advise that a new law is contemplated or a new technology is in development)

  - To exchange opinions (e.g., "If we draft a new law along those lines, would you see any privacy problems with it?" or "Is there any way you can alter that technology so that e-mail traces can still be done if there are legitimate public safety reasons?")

  - To exchange training curricula and modules, training methodology and even trainers

  - To exchange warnings about threats or vulnerabilities

  A suggested first step is to create a list of people and organizations in the country with specific cyberskills and responsibilities in all of the relevant sectors. Contact information for those people can then be noted on the list. It is probably best to keep such a list informal to avoid struggles over who is and who is not on the list.

  In every country, there are likely to be numerous relevant sectors that have a helpful focus on cybersecurity—legislators, ministries, non-governmental organizations, CERTs, academia, the private sector and individuals. Some of these may be wholly domestic and some may be affiliated with larger foreign entities.

- **Develop an understanding among prosecutors, judges and legislators of cybercrime issues.**

  To address cybercrime issues effectively it is important that prosecutors and judges have some understanding of areas such as computers, software and networks, as well as of the increasing importance of electronic evidence. Similarly, legislators should have some understanding of those topics and of whether a country's laws are adequate to address cybercrime. One solution to this problem is training.

  If basic technical training is required, it can come from a variety of sources, depending on the country's resources. They include:

  - Domestic service or ministry with technical competence, such as a law enforcement service or an ICT ministry
  - Foreign governments
  - Relevant multinational organizations
  - The local private sector
  - The international private sector, especially (but not exclusively) if it does business locally
  - Relevant academia
  - Domestic or foreign CERTs
  - Relevant domestic and foreign non-governmental organizations

  It may be helpful to train senior policymakers and government officials on the threats to electronic networks (for example, how the national banking system could be attacked) and about the threats posed by electronic networks (for example, the use of the Internet to locate vulnerable children for sexual trafficking). Training regarding these aspects of electronic networks should be available from the sources above.

  Training may also be desired for prosecutors and judges regarding prosecution of cybercrime or other crime involving electronic evidence, of the use of electronic evidence, or of methods of obtaining international cooperation. Such training may be available from:

  - Domestic service or ministry with the relevant competence, such as a prosecutor's office or a justice ministry
  - Foreign governments
  - Felevant multinational organizations
  - Felevant academia
  - Felevant domestic and foreign non-governmental organizations
  - Felevant individuals

  A country may wish to have training in legislative drafting. Such training may be available from the groups listed in the paragraph above. The local private sector and the international private sector, especially (but not exclusively) if it does business locally, may be possible sources of expertise. However, it is more likely that the private sector entities will be able

to assist with drafting e-commerce laws than with cybercrime, criminal procedure and international mutual legal assistance laws.

For all of these types of training, the sources may offer to deliver the training themselves in the requesting country or they may offer training modules (electronic or printed) that instructors from that country can use in conducting the training themselves. In some cases, such training resources can be provided without charge or with minimal charge.

In some countries, the key to national awareness of cybercrime issues has been the support of senior officials, or sometimes even one powerful senior official, particularly those who control budgets. If it is well-known that a minister is very interested in cybersecurity, his or her ministry—and perhaps the rest of the government—may offer better support to managerial and operational personnel who are trying to accomplish something in the field.

- **Participate in the 24/7 Cybercrime Point of Contact Network.** In 1997, the G8 Subgroup on High-Tech Crime started the 24/7 Cybercrime Point of Contact Network at the direction of the Justice and Interior Ministers of the G8 to improve international assistance in urgent investigations that involve electronic evidence. Many cybercrime investigators felt that it was too difficult to learn where to obtain quick assistance from other countries. In addition, many investigators felt that decades-old mutual legal assistance treaties were not helpful for fast-moving cases involving, for example, midnight computer intrusions into a country's financial systems. The network is open to any country with the necessary capacity to assist as described below:

  - To join the network, countries must offer a contact point reachable twenty-four hours a day, seven days a week, thus the informal name, "the 24/7 network". The contact point can be a person who is reached directly or via an office. He/she must understand three things: (1) technology, so that requests can be transmitted without the delay of lengthy technological explanation; (2) his/her own domestic law; and (3) what domestic law allows him/her to do to assist other countries. If the contact point does not personally have these three types of knowledge, he/she must be able to reach any capable person in his/her government immediately, if necessary (not merely the next business day) who is authorized to assist.

  - Communications must go, at least initially, from the 24/7 contact point in Country A to the 24/7 contact point in Country B to ensure consistency and security. This means that contact points should not give out the contact information to other offices in their own countries. Rather, contact points should make the first international contact on behalf of a requesting office (for example, a provincial law enforcement force) in their countries. After initial cooperation between two countries has been established, a contact point may, if desired, withdraw from the investigation and let the relevant provincial law enforcement in Country A communicate directly with Country B.

  - By joining the network, countries do not guarantee that they will always assist each other, nor does the contact network replace normal mutual legal assistance between countries. Rather, the contact network only guarantees that a requesting country will receive intelligent, capable attention immediately, even in the middle of the night. After any initial assistance, countries may (or may not) require that slower mutual assistance channels be used.

  - Twenty-four-hour-a-day availability does not mean that an office is staffed day and night with a certain number of computer workstations and cyberinvestigators waiting to answer telephone calls or e-mails. Most countries do not operate such an office. More commonly, one law enforcement officer (possibly different officers on a rotating basis) in a country will be reachable by telephone—perhaps sleeping with a mobile phone nearby.

- To join, countries should contact the chair of the High-Tech Crime Subgroup of the G8 (membership is not restricted to G8 members). A short, simple form must be completed. The process does not require formal international agreements such as memoranda of understanding or treaties. From time to time, the 24/7 network offers training and networking conferences for the contact points. Travel to these conferences has been subsidized as needed.

- The unit that joins the network has the responsibility to let local or national law enforcement services or cybercrime units in its country know of its existence and of its availability to assist in making contacts outside the country.

8.3 Case Studies

8.3.1 EU Convention on Cybercrime

The **Convention on Cybercrime**, also known as the **Budapest Convention on Cybercrime**, is the first international treaty seeking to address computer crimes by harmonizing national laws, improving investigative techniques and increasing cooperation among nations. It was drawn up by the Council of Europe in Strasbourg with the active participation of the Council of Europe's observer states, such as Canada, China and Japan.[84]

8.3.2 Korean Cybercrime/Cybersecurity Laws[85]

Act on Digital Signature 1997

The Act on Digital Signature was enacted by the Korea's parliament on July 1997 and revised on 31 December 2005. The purpose of the Digital Signature Act is to promote electronic commerce, with a view to creating a legally predictable environment in which citizens can make secure transactions in the Information Age. The Act endows electronic documents with an equal level of legal validity as paper documents. It also regulates basic matters related to achieving reliability, protecting consumer rights and implementing policies.

Act on Promotion of Utilization of Information and Communication Network and Information Protection 1999

The Act on Promotion of Utilization of Information and Communication Network and Information Protection was enacted on 1999 and revised on December 2007. The purpose of this act is to promote the use of information and communications networks, to protect users' personal information when they are using information and communication services, and to construct an environment within which users can safely use information and communication networks. It was replaced with the new Privacy Protection Act that was enforced in 2011 as described below.

84 Wikipedia, "Convention on Cybercrime". Available at http://en.wikipedia.org/wiki/Convention_on_Cybercrime (accessed on 10 January 2012).

85 This sub-section is drawn heavily from Elgin M. Brunner and Manuel Suter, *International CIIP Handbook 2008 / 2009: An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*, ETH Zurich, Center for Security Studies (2008). Available at http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=91952&lng=en (accessed 10 January 2012). Full text of the acts described below is available at http://www.moleg.go.kr/lawinfo/engLawInfo.

Act on Personal Information Protection for Public Organizations 1994

The Act on Personal Information Protection for Public Organizations, enacted in 1994 and revised in 1998, aims to ensure the adequate performance of public duties, and to protect the rights and interests of users by protecting personal information processed by computers. This act was replaced with the new Privacy Protection Act that was enforced in 2011.

Act on Critical Information Infrastructure Protection 2001

The Act on Critical Information Infrastructure Protection was enacted in January 2001 and revised in December 2007. It serves as a fundamental law protecting critical information infrastructure from various cyberincidents.

Act on Personal Information Protection 2011

The Act on Personal Information Protection, the Republic of Korea's new comprehensive law on data protection, was enacted on 29 March 2011. The recently published regulations (an Enforcement Decree and Enforcement Regulations) apply to any "data processor of personal information" or in short "data processor", which is any entity that uses or processes personal information for business purposes.

e-Commerce Framework

As electronic transactions and commerce across long distances become more common due to the development of ICT networks, a legal framework has been established regarding electronic signatures and their certification, in order to secure the safety and reliability of electronic documents that are drawn up by data processing systems and then transferred, received or saved. The Digital Signature Act and the e-Commerce Framework Act regulate certification of electronic signatures, and the Act on Promotion of Electronic Administration for e-Government governs the use of digital signatures in the public administration.

Summary

- Cybercrimes are offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunications networks such as the Internet (through chat rooms, e-mails, notice boards and groups) and mobile phones (SMS/MMS).

- The types of offences include: offences against the confidentiality, integrity and availability of computer data and systems; content-related offences; copyright-related offences; and computer-related offences.

- Steps to establish cybercrime laws and legislations include:

  - Assessing the current legal authorities for adequacy

  - Drafting and adopting substantive, procedural and mutual assistance laws and policies to address cybercrime

  - Establishing or identifying national cybercrime units

  - Developing cooperative relationships with other elements of the national cybersecurity infrastructure and the private sector

  - Developing an understanding among prosecutors, judges and legislators of cybercrime issues

  - Participating in the 24/7 Cybercrime Point of Contact Network

This chapter can be used by policymakers when they establish a cybercrime registration for their countries.

9. INFORMATION SECURITY MANAGEMENT SYSTEM

You will find in this chapter discussions on:

- **An overview of the information security management system (ISMS);**
- **The ISMS management process;**
- **Requirements for ISMS documentation; and**
- **The information security control structure.**

9.1 Overview

Most public and private organizations have become largely dependent on the ICT infrastructure. As the dependence on the ICT infrastructure increases, cyberattacks on the information assets become more diversified and complicated. The purpose of the ISMS is to design, implement and maintain information security policy in the organizations to manage risks to its information assets, thus, ensuring higher levels of information security.

ISMS certification is increasingly popular around the world, with 2005 as a turning point in the history of internationally standardized ISMS due to the release of two documents: IS 27001, which states the requirements for establishing an ISMS, and IS 17799: 2000, published as IS 17799:2005, which stipulates basic controls for implementing an ISMS.

Most accredited certification bodies are certifying according to ISO/IEC 27001. In some countries, the bodies that verify conformity of management systems to specific standards are called “certification bodies”, while in others they are commonly referred to as “registration bodies”, “assessment and registration bodies”, “certification/registration bodies”, and sometimes “registrars”. Certification against any of the recognized national variants of ISO/IEC 27001 bodies is functionally equivalent to certification against ISO/IEC 27001 itself.

Audit for ISO/IEC 27001 certification is conducted in three stages. The first stage is an informal review of the ISMS. At this stage, the ISMS auditors check the existence and completeness of key documents, such as the organization’s information security policy, Statement of Applicability and Risk Treatment Plan. The second stage is to test the ISMS requirements specified in ISO/IEC 27001. The evaluators will confirm that the ISMS in the organization has been appropriately designed and implemented based on ISO/IEC 27001 standards. Passing this stage, the ISMS certification is granted to the ISMS applicants.

According to the ISMS international user group, ISO/IEC issued a total of 7,346 ISMS certifications to 87 countries as of November 2011. The following are countries with the highest number of certifications: Japan (3,862), UK (534), India (527), China (494), Taiwan (451), Germany (181), Czech Republic (111), Republic of Korea (106) and USA (104).

The third stage is follow-up activities after certification. Certification maintenance makes sure that the certificated ISMS is working as specified and intended. Follow-up activities are conducted at least annually but can take place more frequently during the initial years of ISMS certification.

9.2 ISMS Management Process

ISMS implementation consists of managing process, documentation requirements, and the control clauses to check the establishment and operation of the ISMS.

The ISMS uses a process approach for establishing, implementing and operating, monitoring and reviewing, maintaining and improving the ISMS in the organization. The process approach emphasizes the following:

- Understanding the need to establish an ISMS
- Implementing and operating an ISMS to manage overall business risks in the organization
- Monitoring and reviewing the performance and effectiveness of the ISMS regularly
- Implementing the identified improvements in the ISMS

All ISMS processes adopt the "Plan-Do-Check-Act" model, (see table 4). The model shows how an ISMS takes as input the information security requirements and expectations of the interested parties and through the necessary actions and processes produces information security outcomes that meets those requirements and expectations.

Table 4. "Plan-Do-Check-Act" cycle of the ISMS

Level	Goal	Contents
Plan	Establish the ISMS	• Definition of the scope • Risk analysis • Security policy development • Risk management plan
Do	Implement and operate the ISMS	• Security policy implementation • Application of controls • Process integration • Implement training
Check	Monitor and review the ISMS	• Monitoring • Incident documentation • Review effectiveness • Identify non-conformities • Identify new/changed risks
Action	Maintain and improve the ISMS	• Implement improvements • Control non-conformities • Review risk analysis • React to changed risks

Source: ISO/IEC 27001, first edition (2005).

9.3 Documentation Requirements

The ISMS documentation is necessary to confirm the selected controls to the results of the risk assessment and risk treatment process, and subsequently back to the ISMS policy and objectives. ISO/IEC 27001 puts emphasis on the recording of management decisions, control of documents and control of records.[86]

Firstly, documentation should include records of management decisions, and the Information Security Officer should keep records of the following:

- Documented statements of the ISMS policy and objectives
- The scope of the ISMS

86 ISO/IEC 27001 information technology – security techniques – information security management system – requirements (15 October 2005).

- Procedures and controls in support of the ISMS
- A description of the risk assessment methodology
- The risk assessment report
- The risk treatment plan
- Documented procedures needed by the organization to ensure the effective planning, operation and control of its information security processes, and descriptions of how the effectiveness of controls are measured
- Records required by the ISO
- The Statement of Applicability

Secondly, all documents required by the ISMS should be protected and controlled as follows:

- Review and approve documents
- Review and update documents
- Identify update and the current revision status of documents
- Distribute and control relevant versions of applicable documents
- Prevent the unintended use of obsolete documents

Thirdly, the controls needed for the identification, storage, protection, retrieval, retention time and disposition of records should be documented and implemented, and remain legible, readily identifiable and retrievable.

9.4 Information Security Control Structure

The ISMS is comprised of 11 security control items, the categories of each control item are as follows:[87]

Information Security Policy

The information security policy outlines the organization's direction on information security. The policy should be developed with top management in accordance with business requirements and relevant laws and regulations. The information security policy document should be approved and published by top management, and the policy should be reviewed if significant changes occur to ensure its suitability, adequacy and effectiveness.

Organization of Information Security

An organizational structure for information security should be established to initiate and control the implementation of information security within an organization. To achieve this, top management should approve security direction, assign roles, and coordinate and review the implementation of information security within the organization. Information security responsibility should be clearly assigned, and authorization process for new information processing facilities should be defined and implemented.

87 Ibid.

Asset Management

Asset management is to achieve and maintain protection of organizational assets by the inventory and classification of information assets. All assets should be allocated responsibilities and classified to indicate the priorities of the organization's assets.

Human Resources Security

Human resources security is to minimize the risks by theft, fraud and misuse in the security aspects for employees joining, moving and leaving an organization. Security procedures for human resources can be classified according to prior to employment, during employment, termination and change of employment.

Physical and Environmental Security

Physical and environmental security is to prevent unauthorized physical access, damage and interference to an organization's ICT facilities. These measures consist of secure areas and equipment security.

Communications and Operations Management

Communications and operations management is the management of technical security controls to ensure the correct and secure operation of information processing facilities. This measure consists of 10 control items: documented operating procedures, third party service delivery management, system planning and acceptance, protection against malicious and mobile code, back-up, network security management, media handling, exchanges of information, e-commerce services and monitoring.

Access Control

Access control means the restriction of access rights to networks, systems, applications, functions and data. The measures for access control consist of seven control items: business requirement for access control, user access management, user responsibility, network access control, operating system access control, application and information access control, and mobile computing and teleworking.

Information Systems Acquisition, Development and Maintenance

These measures are to ensure that information security is an integral part of information systems and consist of six control items: security requirements analysis and specification, correct processing in application, cryptographic controls, security of system files, security in development and support processes, and technical vulnerabilities management.

Information Security Incident Management

Information security incident management is to anticipate and respond appropriately to information security breaches, report information security events and weakness, and manage information security incidents and improvement.

Business Continuity Planning

Business continuity planning is planning that identifies the organization's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for the organization, whilst maintaining a competitive advantage and value system integrity.

Compliance

Compliance means ensuring conformance with information security policies, standards, laws and regulations. Due to the increasing number of regulations and need for operational transparency, organizations are increasingly adopting the use of consolidated and harmonized sets of compliance controls. Compliance consists of three control items: compliance with legal requirements; compliance with security policies, standards and technical requirements; and information system audit considerations.

9.5 Case Study from the Republic of Korea

In the Republic of Korea, KISA began independent K-ISMS based on international standards in February 2002. Since then, the K-ISMS' certification has been issued to 115 Korean companies as of September 2011. K-ISMS consists of 15 clauses, adding outsider control, information asset classification, education, control to controls in ISO/IEC 27002. And 15 clauses are separated into 48 categories.

In addition, Korean G-ISMS for the central and local government began in December 2009. G-ISMS based on ISO 27001 consists of 12 clauses including personal information protection and 44 categories.

Summary

- The ISMS consists of processes and systems to ensure confidentiality, integrity and availability of information assets while minimizing security risks.
- Most accredited certification bodies are certifying the ISMS according to ISO/IEC 27001. The certification process of ISMS consists of three stages. The first stage is to familiarize the evaluators with the organization. The second stage is to test the ISMS requirements specified in ISO/IEC 27001. The third stage includes follow-up activities after certification.
- Applicants of ISMS certification need to establish and implement a managing process, documentation requirements and control structure.
- ISMS documentation is necessary to confirm the selected controls to the results of the risk assessment and risk treatment process, and subsequently back to the ISMS policy and objectives. The ISO/IEC 27001 places emphasis on the recording of management decisions, control of documents and control of records.
- The control structure of the ISMS standard consists of 11 security control items: information security policy; organization of information security; asset management; human resources security; physical and environmental security; communications and operations management; access control; information systems acquisition, development and maintenance; information security incident management; business continuity planning; and compliance.

This chapter can be used by policymakers to promote ISMS certification, or when organizations establish an ISMS.

ANNEX CHARACTERISTICS AND CLASSIFICATION OF CYBERCRIME

1. Offences against the Confidentiality, Integrity and Availability of Computer Data and Systems

All offences in this category are directed against (at least) one of the three legal principles of confidentiality, integrity and availability. They are composed of illegal access, illegal data acquisition, illegal interception, data interference and system interference.

Illegal Access (Hacking, Cracking)

Illegal access described as “hacking” refers to unlawful access to a computer system or information, one of the traditional computer-related crimes. Following the development of computer networks (especially the Internet), this crime has become a mass phenomenon. Famous targets of hacking attacks include government agencies, public organizations, major Internet portals, private sector and e-transaction sites on the Internet.

Illegal Data Acquisition (Data Espionage)

Sensitive information is often stored in computer systems. If the computer system is connected to the Internet, offenders can try to access this information via the Internet from almost any place in the world. The Internet is increasingly used to obtain trade secrets. The value of sensitive information and the ability to access it remotely makes data espionage highly interesting. Offenders use various techniques to access victims’ computers, including software to scan for unprotected ports or circumvent protection measures, as well as “social engineering”. Social engineering is usually very successful, because the weakest link in computer security is often the users operating the computer system. One example is “phishing”, which has recently become a key crime committed in cyberspace and describes attempts to fraudulently acquire sensitive information (such as passwords) by masquerading as a trustworthy person or business (e.g., financial institution) in a seemingly official electronic communication.

Illegal Interception

Offenders can intercept communication between users (such as e-mails) or other forms of data transfers (when users upload data onto Web servers or access Web-based external storage media in order to record the information exchanged. In this context, offenders can in general target any communication infrastructure (e.g., fixed lines or wireless) and any Internet service (e.g., e-mail, chat or Voice over Internet Protocol [VoIP] communications).

Most data transfer processes among Internet infrastructure providers or Internet service providers are well protected and difficult to intercept. However, offenders search for weak points in the system. Wireless technologies are enjoying greater popularity and have in the past proved vulnerable. Nowadays, hotels, restaurants and bars offer customers Internet access through wireless access points. However, the signals in the data exchanges between the computer and the access point can be received within a radius of up to 100 metres.

Most countries have moved to protect the use of telecommunications services by criminalizing the illegal interception of phone conversations. However, given the growing popularity of IP-based services, lawmakers may need to evaluate to what extent similar protection is offered to IP-based services.

Data Interference

Computer data are vital for private users, businesses and administrations, all of which depend on the integrity and availability of data. Lack of access to data can result in considerable (financial) damage. Offenders can violate the integrity of data and interfere with them by deleting, suppressing or altering computer data. One common example of the deletion of data is the computer virus.

System Interference

The same concerns over attacks against computer data apply to attacks against computer systems. More businesses are incorporating Internet services into their production processes, with benefits of 24-hour availability and worldwide accessibility. If offenders succeed in preventing computer systems from operating smoothly, this can result in great financial losses for victims. More challenging for legal systems are Web-based scams. Examples of these remote attacks against computer systems include computer worms and DoS attacks.

Computer worms are a subgroup of malware (e.g., computer viruses). They are self-replicating computer programs that harm the network by initiating multiple data transfer processes. They can influence computer systems by hindering the smooth running of the computer system, using system resources to replicate themselves over the Internet or generating network traffic that can close down availability of certain services (such as websites).

While computer worms generally influence the whole network without targeting specific computer systems, DoS attacks target specific computer systems. A DoS attack makes computer resources unavailable to their intended users. By targeting a computer system with more requests than the computer system can handle, offenders can prevent users from accessing the computer system, checking e-mails, reading the news, booking a flight or downloading files. DDoS attacks were reported in 2009 on government and commercial websites in the Republic of Korea and the USA. As a result, some of the services were not available for several hours and even days. The prosecution of DoS and computer-worm attacks poses serious challenges to most criminal law systems, as these attacks may not involve any physical impact on computer systems. Apart from the basic need to criminalize Web-based attacks, the question of whether the prevention and prosecution of attacks against critical infrastructure needs a separate legislative approach is under discussion.

2. Content-Related Offences

Erotic or Pornographic Material (excluding Child Pornography)

Sexually-related content was among the first content to be commercially distributed over the Internet, which offers advantages to retailers of erotic and pornographic material including:

- Exchange of media (such as pictures, movies, live coverage) without the need for cost-intensive shipping
- Worldwide access, reaching a significantly larger number of customers than retail shops
- The Internet being often viewed as an anonymous medium (often erroneously)—an aspect that consumers of pornography appreciate, in view of prevailing social opinions

Child Pornography

The Internet has become a prime channel for the distribution of child pornography. In the 1970s and 1980s, offenders engaging in the exchange of child pornography faced serious threats.

Racism, Hate Speech, Glorification of Violence

Radical groups use mass communication systems such as the Internet to spread propaganda. The number of websites offering racist content and hate speech are on the rise in recent years—a study in 2005 suggested a rise of 25 per cent in the number of Web pages promoting racial hatred, violence and xenophobia between 2004 and 2005. In 2006, over 6,000 such websites existed on the Internet.

Internet distribution offers several advantages for offenders, including lower distribution costs, non-specialist equipment and a global audience. Examples of incitement to hatred websites include websites presenting instructions on how to build bombs. Besides propaganda, the Internet is used to sell certain goods, e.g., Nazi-related items such as flags with symbols, uniforms and books are readily available on auction platforms and specialized Web shops. The Internet is also used to send e-mails and newsletters and distribute video clips and television shows through popular archives such as YouTube.

Not all countries may criminalize these offences. In some countries, such content may be protected by principles of freedom of speech.

3. Religious Offences

A growing number of websites present materials that are in some countries covered by provisions related to religious offences (e.g., written anti-religious statements). Although some materials document objective facts and trends (e.g., decreasing church attendance in Europe), this information may be considered illegal in some jurisdictions. Other examples include the defamation of religions or the publication of cartoons.

Illegal Gambling and Online Games

Internet games and gambling are one of the fastest-growing areas on the Internet.

Libel and False Information

The Internet can be used to spread misinformation just as easily as information. Websites can present false or defamatory information, especially in forums and chat rooms, where users can post messages without verification by moderators.

Spam and Related Threats

“Spam” describes the emission of unsolicited bulk messages. Although various scams exist, the most common one is e-mail spam. Offenders send out millions of e-mails to users, often containing advertisements for products and services, but frequently also malicious software.

Other Forms of Illegal Content

The Internet is not only used for direct attacks, but also as a forum for soliciting, offers and incitement to commit crimes, unlawful sale of products, and providing information and instructions for illegal acts (e.g., how to build explosives).

4. Copyright- and Trademark-Related Offences

Copyright-Related Offences

Digitization has enabled the entertainment industry to add additional features and services to movies on DVD, including languages, subtitles, trailers and bonus material. CDs and DVDs have proved more sustainable than records and videotapes.

Trademark-Related Offences

Trademark violations, a well-known aspect of global trade, are similar to copyright violations. Violations related to trademarks have transferred to cyberspace, with varying degrees of criminalization under different national penal codes.

5. Computer-Related Offences

Fraud and Computer-Related Fraud

Computer-related fraud is one of the most popular crimes on the Internet, as it enables the offender to use automation and software tools to mask criminals’ identities.

Computer-Related Forgery

Computer-related forgery describes the manipulation of digital documents. The offence can for example be committed by creating a document that appears to originate from a reliable institution, manipulating electronic images (for example, pictures used as evidence in court) or altering text documents.

Identity Theft

The term identity theft—which is neither consistently defined nor consistently used—describes the criminal act of fraudulently obtaining and using another person’s identity. These acts can be carried out without the help of technical means as well as online by using Internet technology.

Misuse of Devices

Cybercrime can be committed using only fairly basic equipment. Committing offences such as libel or online fraud needs nothing more than a computer and Internet access and can be carried out from a public Internet café. More sophisticated offences can be committed using specialist software tools.

6. Combination Offences

Terrorist Use of the Internet

In the 1990s, discussion about the use of the network by terrorist organizations focused on network-based attacks against critical infrastructure such as transportation and energy supply ("cyberterrorism") and the use of ICTs in armed conflicts ("cyberwarfare"). The success of virus and botnet attacks has clearly demonstrated weaknesses in network security. Successful Internet-based attacks by terrorists are possible, but it is difficult to assess the significance of threats. Back then, the degree of interconnection was small compared to nowadays, and it is very likely that this—apart from the interest of the states to keep successful attacks confidential—is one of the main reasons why such incidents were rarely reported.

Cyberwarfare

After the attacks against computer systems in Estonia in 2007 and Georgia in 2008 and more recently after the discovery of the "Stuxnet" worm, which is believed to have secretly targeted specific equipment used in Iran's nuclear programme, the term cyberwarfare has frequently been employed to describe the situation although the use of terminology is problematical.

Cyberlaundering

The Internet is transforming money laundering. For larger amounts, traditional money laundering techniques still offer a number of advantages, but the Internet offers several advantages. Online financial services offer the option of processing multiple, worldwide financial transactions very quickly. The Internet has helped overcome the dependence on physical monetary transactions. Wire transfers replaced the transport of hard cash as the original first step in suppressing physical dependence on money, but stricter regulations to detect suspicious wire transfers have forced offenders to develop new techniques. The detection of suspicious transactions in the fight against money laundering is based on obligations of the financial institutions involved in the transfer.

Phishing

Offenders have developed techniques to obtain personal information from users, ranging from spyware to phishing attacks. Phishing describes acts that are carried out to make victims disclose personal/secret information. There are different types of phishing attacks, but e-mail-based phishing attacks contain three major phases. In the first phase, offenders identify legitimate companies offering online services and communicating electronically with customers whom they can target (e.g., financial institutions). Offenders design websites resembling the legitimate websites (spoofing sites) requiring victims to perform normal log in procedures, enabling offenders to obtain personal information (e.g., account numbers and online banking passwords).

UNITED NATIONS
APCICT - ESCAP

Bonbudong, 3rd Floor Songdo Techno Park,
7-50 Songdo-dong, Yeonsu-gu, Incheon City, Korea
Tel: +82 32 245 1700-2 Fax: +82 32 245 7712
www.unapcict.org

ISBN 978-89-959820-1-3