Information Security and Privacy

Academy of ICT Essentials
for Government Leaders

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

The Academy of ICT Essentials for Government Leaders

Information Security and Privacy

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

Academy of ICT Essentials for Government Leaders

Information Security and Privacy

Disclaimers: The views expressed herein are those of the authors, and do not necessarily reflect the views of the United Nations. This publication has been issued without formal editing, and the designations employed and material presented do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

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

Correspondence concerning this report should be addressed to the email: apcict@un.org

Printed in Republic of Korea
ST/ESCAP/2934

Cover design: Mr. Ho-Din Ligay

Contact:

Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT/ESCAP)
5th Floor G-Tower, 175 Art Center Daero
Yeonsu-gu, Incheon, Republic of Korea
Tel +82 32 458 6650

Email: apcict@un.org

ABOUT THE MODULE SERIES

In today's "Information Age", easy access to information is changing the way we live, work and play. The "digital economy", also known as the "knowledge economy", "networked economy" or "new economy", is characterized by a shift from the production of goods to the creation of ideas. This underscores the growing, if not already central, role being played by information and communication technologies (ICTs) in the economy, in particular, and in society as a whole.

As a consequence, governments worldwide have increasingly focused on ICTs for development (ICTD). For these governments, ICTD is not only about developing the ICT industry or sector of the economy, but also encompasses the use of ICTs to stimulate economic growth, as well as social and political development.

However, among the difficulties that governments face in formulating ICT policy is unfamiliarity with a rapidly changing technology landscape and the competencies needed to harness ICTs for national development. Since one cannot regulate what one does not understand, many policymakers have shied away from ICT policymaking. But leaving ICT policy to technologists is also wrong because often, technologists are unaware of the social and policy implications of the technologies they are developing and using.

The Academy of ICT Essentials for Government Leaders module series has been developed by the Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT) for:

1. Policymakers at the national and local government level who are responsible for ICT policymaking;
2. Government officials responsible for the development and implementation of ICT-based applications; and
3. Managers in the public sector seeking to employ ICT tools for project management.

The module series aims to develop familiarity with the substantive issues related to ICTD from both a policy and technology perspective. The intention is not to develop a technical ICT manual. Rather, its purpose is to provide a good understanding of what the current digital technology is capable of achieving and where technology is headed, and what this implies for policymaking. The topics covered by the modules have been identified through a training needs analysis and a survey of other training materials worldwide.

The modules are designed in such a way that they can be used for self-study by individuals or as a resource in a training course or programme. The modules are stand-alone as well as linked together, and effort has been made in each module to link to themes and discussions in the other modules in the series. The long-term objective is to make the modules a coherent course that can be certified.

Each module begins with a statement of module objectives and target learning outcomes against which readers can assess their own progress. The module content is divided into sections that include case studies and exercises to help deepen understanding of key concepts. The exercises may be done by individual readers or by groups of training participants. Figures and tables are provided to illustrate specific aspects of the discussion. References and online resources are listed for readers to look up in order to gain additional perspectives.

The use of ICTD is so diverse that sometimes case studies and examples within and across modules may appear contradictory. This is to be expected. This is the excitement and the challenge of this discipline and its promise, as countries leverage the potential of ICTs as tools for development.

Supporting the Academy of ICT Essentials for Government Leaders module series in print format is an online distance learning platform ─ the APCICT Virtual Academy (http://e-learning.unapcict.org) ─ with virtual classrooms featuring the trainers' presentations in video format and PowerPoint presentations of the module.

ACKNOWLEDGEMENTS

The Academy of ICT Essentials for Government Leaders: Information Security and Privacy was prepared by Freddy Tan, under the overall guidance of Kiyoung Ko, Director of Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT). The module was coordinated by Robert De Jesus.

The module benefited from substantive comments of participants to the Consultative Meeting on Capacity Building for Digital Development, held on 27-28 November 2019, in Incheon. Additional reviews and inputs were also provided by the International Telecommunications Union (ITU) and the Information and Communications Technology and Disaster Risk Reduction Division (IDD) of ESCAP.

The cover design was created by Ho-Din Ligay and the layout was provided by Angielika Bartolome and Gyubin Hwang. Sze-shing Poon and Sara Bennouna proofread the manuscript. Joo-Eun Chung and Ho-Din Ligay undertook all administrative processing necessary for the issuance of this module.

MODULE OBJECTIVES

The module aims to:

1. Clarify the concept of information security, privacy and related concepts;

2. Describe threats to information security and how they can be addressed;

3. Discuss the requirements for the establishment and implementation of policy on information security, as well as the life cycle of information security policy; and

4. Provide an overview of standards of information security and privacy protection that are used by some countries and international information security organizations.

LEARNING OUTCOMES

After working on this module, users should be able to:

1. Define information security, privacy and related concepts;

2. Identify threats to information security;

3. Assess existing information security policy in terms of international standards of information security and privacy protection; and

4. Formulate or make recommendations regarding information security policy that would be appropriate to their own context.

Table of Contents

List of Tables

List of Figures

List of Boxes

List of Case Studies

1. Need for Information Security

This section aims to:

Explain the concept of information and information security; and
Describe standards applied to information security activities

Human life today is highly dependent on information and communications technology (ICT). This makes individuals, organizations and nations highly vulnerable to attacks on information systems, such as cyber-intrusions, cyber-terrorism, cyber-crime, and the like. Few individuals and organizations are equipped to cope with such attacks. Governments have an important role to play in ensuring information security by expanding the information-communication infrastructure and establishing systems to protect against information security threats.

This module focuses on Information Security which is part of Cyber Security. Issues on freedom of expression online, human rights online, violence against women and girls (VAWG) online, digital abuse and online sexual harassment, hate speech online, cyberbullying, and child online protection (COP) initiatives have been excluded in this module, and they can form part of a separate module on Internet/Online safety awareness.

1.1. Basic Concepts in Information Security

What is information?

Generally, information is defined as the result of mental activity; it is an intangible product that is transmitted through media. In the field of ICT, information is the result of processing, manipulating and organizing data, which is simply a collection of facts.

In the field of Information Security, information is defined as an “asset”; it is something that has value and should therefore be protected. The definition of information and information security in ISO/IEC 27001:2005 is used throughout this module.

The value assigned to information today reflects the shift from an agricultural society to an industrial society and finally to an information-oriented society. In agricultural societies, land was the most important asset and the country with the largest production of grain had a competitive edge. In industrial societies, capital strength, such as having oil reserves, was a key factor in competitiveness. In a knowledge and information-oriented society, information is the most important asset and the ability to collect, analyze and use information is a competitive advantage for any country.

As the perspective has shifted from net asset value to information asset value, there is a growing consensus that information needs to be protected. Information itself is valued more than the media holding information. Table 1 contrasts information assets with tangible assets.

As shown in table 1, information assets are radically different from tangible assets. Thus, information assets are vulnerable to different kinds of risks.

Table 1

Characteristic	Information assets	Tangible assets
Form – maintenance	Have no physical form and can be flexible	Have physical form
Value – variableness	Attain higher value when combined and processed	Total value is the sum of each value
Sharing	Unlimited reproduction of information assets is possible, and people can share the value	Reproduction is impossible; with reproduction, the value of the asset is reduced
Media – dependency	Need to be delivered through media	Can be delivered independently (due to their physical form)

Risks to information assets

As the value of information assets goes up, the desire to gain access to information and to control it increases among people. Groups are formed to use information assets for various objectives, and some exert effort to obtain information assets by whatever means. The latter include unauthorized access (hacking), unauthorized use (piracy), destruction of information systems through computer viruses, and others. These risks that are attendant on informatization are discussed in section 2 of this module.

The negative aspects of information-oriented environments include the following:

Increase in unethical behavior arising from anonymity – ICT can be used to maintain anonymity, which makes it easy for certain individuals to engage in unethical and criminal behavior, including illegal acquisition of information.

Conflicts over ownership and control of information – Complications caused by ownership and control of information have increased with the expansion of informatization. For example, as governments seek to build a personal information database under the umbrella of e-government, some sectors have expressed concern over the possibility of invasion of privacy from the disclosure of personal information to other parties.

Information and wealth gaps between classes and countries – The size of information asset holdings can be the barometer of wealth in knowledge/information-oriented societies. Developed countries have the capacity to produce more information and to profit from selling information as products. Information-poor countries, by contrast, need huge investments just to be able to access information.

Growing information exposure caused by advanced networks – The knowledge/information-oriented society is a network society. The whole world is connected like a single network, which means that weaknesses in one part of the network can adversely impact the rest of the network.

What is information security?

Information security is defined as the preservation of confidentiality, integrity and availability of information.[1] It typically involves preventing or at least reducing the probability of unauthorized/inappropriate access, use, disclosure, disruption, deletion/destruction, corruption, modification, inspection, recording or devaluation, although it may also involve reducing the adverse impacts of incidents. Information may take any form, e.g., electronic or physical, tangible (e.g. paperwork) or intangible (e.g. knowledge).

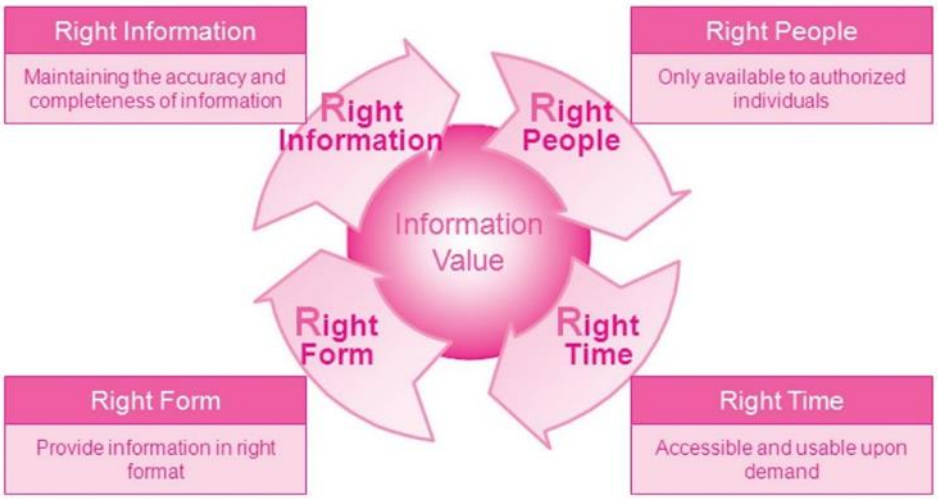
Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity.

Cyber Security, in contrast, includes not only information security, but also digital infrastructure security, such as Supervisory Control and Data Acquisition (SCADA) systems and Internet-of-Things (IoT) systems, which goes beyond the protection of valuable information.

4Rs of information security

The 4Rs of information security are Right Information, Right People, Right Time and Right Form. Control over the 4Rs is the most efficient way to maintain and control the value of information.

Figure 1: 4Rs of Information Security



"Right Information" refers to the accuracy and completeness of information, which guarantees the integrity of information.

[1] International Organization for Standardization. (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary (ISO/IEC Standard No. 27000). Retrieved from https://www.iso.org/standard/73906.html

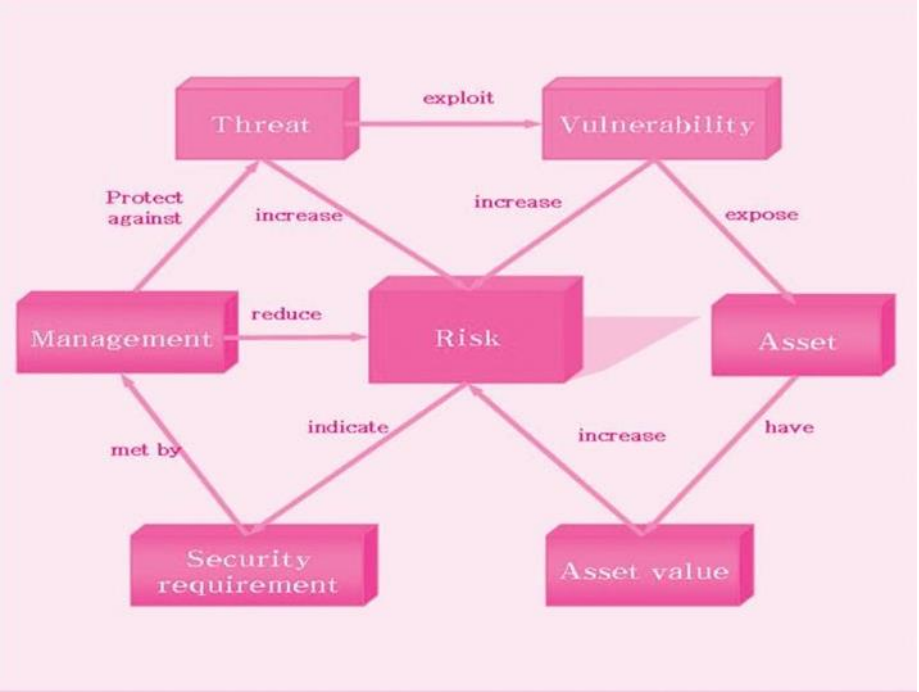
“Right People” means that information is available only to authorized individuals, which guarantees confidentiality.

“Right Time” refers to the accessibility of information and its usability upon demand by an authorized entity. This guarantees availability.

“Right Form” refers to providing information in the right format.

To safeguard information security, the 4Rs have to be applied properly. This means that confidentiality, integrity and availability should be observed when handling information.

Figure 2: Correlation between risk and information assets



Information security also requires a clear understanding of the value of information assets, as well as their vulnerabilities and corresponding threats. This is known as risk management. Figure 2 above shows the correlation between information assets and risk.

Risk is determined by the asset value, threats and vulnerabilities. The formula is as follows:
Risk = ∫(Asset Value, Threats, Vulnerabilities)

Risk is directly proportional to asset value, threats and vulnerabilities. Thus, the risk can be increased or decreased by manipulating the size of the asset value, threats and vulnerabilities. This can be done through risk management.
The methods of risk management are as follows:

Risk reduction (risk mitigation) – This is done when the likelihood of threats/vulnerabilities is high, but their effect is low. It involves understanding what the threats and vulnerabilities are, altering or reducing them, and implementing a countermeasure. However, risk reduction does not reduce the value of risk to “0”.

Risk acceptance – This is done when the likelihood of threats/vulnerabilities is low and their likely impact is minor or acceptable.

Risk transference – If the risk is excessively high or the organization is not able to prepare the necessary controls, the risk can be transferred outside of the organization. An example is taking out an insurance policy.

Risk avoidance – If the threats and vulnerabilities are highly likely to occur and the impact is also extremely high, it is best to avoid the risk by outsourcing data processing equipment and staff, for example.

Figure 3: Methods of Risk Management

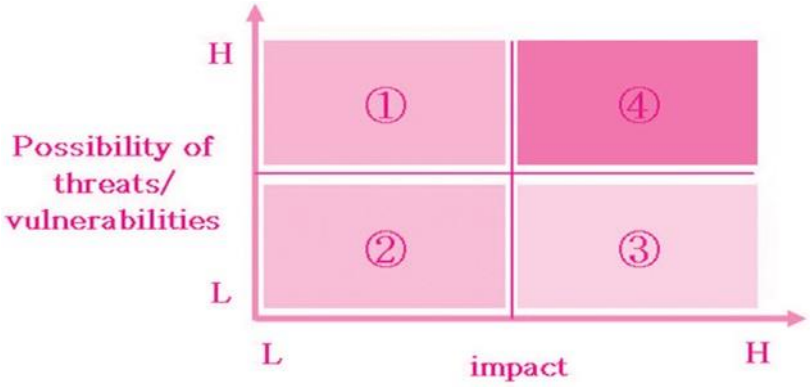


Figure 3 above is a graphic representation of these four methods of risk management. In this figure, the quadrant marked "1" is risk reduction, "2" is risk acceptance, "3" is risk transference and "4" is risk avoidance.

A key consideration in choosing the appropriate risk management method is cost-effectiveness. A cost-effectiveness analysis should be performed before the plan for risk reduction, acceptance, transference, or avoidance is established.

1.2. Standards for Information Security Activities

Information security activities cannot be effectively performed without the mobilization of a unified administrative, physical and technical plan.

Many organizations have recommended standards for information security activities. Examples include the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC), International Telecommunication Union (ITU-U), information security requirements and evaluation items of the Certified Information Systems Auditor (CISA) of the Information Systems Audit and Control Association (ISACA), and Certified Information Systems Security Professional (CISSP) of the International Information System Security Certification Consortium (ISC)[2]. These standards recommend unified

[2] (ISC)². (2020). Cybersecurity Certification: CISSP - Certified Information Systems Security Professional: (ISC) http://www.isc2.org/cissp

information security activities, such as the formulation of an information security policy, the construction and operation of an information security organization, human resources management, physical security management, technical security management, security audit and business continuity management.

Table 2 lists the standards related to information security domains.

Table 2: Information security domains and related standard and certifications

Security domains	ISO/IEC 27001	CISA	CISSP
Administrative	Information Security Policy	Governance and Management of IT	Security Architecture and Engineering
	Organization of Information Security		
	Asset Management	Protection of Information Assets	Security and Risk Management
	Human Resources Security		
	Information Security Incident Management		
	Information Security aspects of Business Continuity Management		
	Supplier Relationships Compliance	Information systems (IS) Auditing Process	Security Assessment and Testing
Physical	Physical and Environmental Security		Asset Security
Technical	Cryptography Communications Security Operations Security	Information Systems Operations and Business Resilience	Security Operations Communications and Network Security
	Access Control		Identity and Access Management

	System Acquisition, Development and Maintenance	Information Systems Acquisition, Development and Implementation	Software Development Security

ISO/IEC27001 focuses on administrative security. In particular, it emphasizes documentation and operation audit as administrative behavior and the observance of policy/guideline and law. Continuous confirmation and countermeasures by the administrator are required. Thus, ISO/IEC27001 tries to address the weak points of security systems, equipment, and the like in an administrative way.

In contrast, there is no mention of human resources or physical security in CISA, which focuses on audit activities and controls on information systems. Accordingly, the role of auditors and the performance of audit process are considered very important.

CISSP[3] focuses mainly on technical security. It emphasizes the software development, identity and access management, communications and network security and operations security.

Something to Do:

1. Assess the level of information security awareness among members of your organization.

2. What information security measures does your organization implement? Classify these measures in terms of the four methods of information security.

3. Identify examples of information security measures in the administrative, physical and technical domains within your organization or in other organizations in your country or jurisdiction.

Training participants can do this exercise in small groups. If participants come from different countries, the small groups can be by country.

[3] Ibid.

Test Yourself:

1. How is information different from other assets?
2. Why is information security a concern for policy makers?
3. What are ways of ensuring information security? Differentiate the various methods of addressing information security.
4. Differentiate between each of the three information security domains (administrative, physical and technical).

2. Information Security Trends and Directions

This section aims to:

Provide an overview of threats to information security; and
Describe countermeasures against such threats

2.1. Types of Cyber Threats

External Threats

External threats are attacks that are conducted from non-employees and the attacks are usually done remotely from outside the organization's office. Examples of such threats include hacking, denial of service and malware.

Internal Threats

Internal threats are attacks that are conducted by employees or contractors who have physical access to the organization's systems, networks and applications. Such attacks are usually carried out by disgruntled employees/contractors. Internal attacks can also be unknowingly facilitated by employees/contractors using social engineering and exploiting less security aware employees.

2.2. Types of External Threats

Hacking

Hacking is the act of gaining access to a computer or computer network to obtain or modify information without legal authorization.

Hacking can be classified as recreational, criminal or political hacking, depending on the purpose of the attack. Recreational hacking is unauthorized modification of programs and data simply to satisfy the hacker's curiosity. Criminal hacking is used in fraud or espionage. Political hacking is tampering with websites to broadcast unauthorized political messages.

Recently, hacking[4] has become more and more implicated in cyber terrorism and cyberwarfare, posing a major threat to national security. Another new trend shows hacking groups targeting major sites with national interest and holding highly sensitive information.

[4] Cross, D. (2017, January 10). *World's Most Recent & Biggest Hacking Incidents*. Web Hosting Media. https://webhostingmedia.net/recent-biggest-hacking-incidents.

Box 1: Some examples of criminal and recreational hacking

The JPMorgan Chase Bank Hacked

More than 80 million user accounts got revealed to hackers in 2014.

A Russian hacker group has hit one of the largest banks in the United States of America. They managed to breach 76 million personal accounts and 7 million small business accounts. They infiltrated all 90 of JPMorgan Chase's server computers and were able to view all the personal information of the account holders.

The hackers stole basic information, such as names, phone numbers, email addresses and home addresses.

Denial-of-Service and Distributed Denial-of-Service

Denial-of-Service (DoS) causes an action upon a computer or networked device that results in other processes, resources or activities floundering and failing to respond adequately. Distributed Denial-of-Service (DDoS) attacks are where multiple participating devices engage in DoS attacks from a distributed assortment of location.

The specific attack traffic or vulnerability exploitation that causes the target(s) to become unresponsive is typically the same for both DDoS and DoS attacks. The distributed sources engaged in the DDoS attack often make the attack more difficult to defend against and are generally more successful against larger and faster responding targets.[5]

Case Study 1: Global websites suffering DDoS attack

Email Spam

Spam is a bulk, unsolicited, commercial electronic message delivered through information communication service such as e-mail. Spam is a low-cost and effective medium for advertising. Recently, spam has been used to spread malicious code or seize personal information. Sometimes, this type of spam is sent from zombie PCs that are, in most cases, infected by malicious codes.

In October 2016, cybercriminals launched major DDoS attacks, disrupting a host of websites, including Twitter, Netflix, PayPal, Pinterest and the PlayStation Network, amongst many others.

The attack was staggering for its size, at one time measuring close to 1 Tbps. The group behind the attack did this by compromising twenty thousand of endpoint IoT devices, transforming them in a botnet and essentially flooding traffic to DNS hosting provider Dyn.

Source (with modification): https://www.welivesecurity.com/2016/12/30/biggest-security-incidents-2016/.

[5] SecureAuth. (2017, July 14). secureauth_ciam_infographic_170714.pdf. Irvine.

Case Study 2: World's biggest source of spam email shut down

The Rustock botnet, an international network of virus-infected computers, had for years generated billions of emails per day, promoting unlicensed online pharmacies and cut-price impotence pills.

In March 2011, Microsoft, backed by US Marshals acting on a court order, seized servers that it was estimated covertly controlled almost a million Windows PCs.

The servers were rented from commercial internet hosting firms across the Mid-West, which were apparently unaware of their role in Rustock. These "command and control" servers would issue instructions to infected home and business PCs worldwide.

Source (with modification): https://www.telegraph.co.uk/technology/news/8391532/Worlds-biggest-source-of-spam-email-shut-down.html.

Phishing

Phishing is the use of email or messages to obtain sensitive information such as usernames, passwords and credit card details by using a trustworthy entity. It is typically carried out by email spoofing or instant messaging, and it often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site.

Case Study 3: The United Kingdom's biggest ever cyber fraud

The United Kingdom Metropolitan Police's Action Fraud unit estimated that £59m worth of fraud was prevented in the United Kingdom after three men were convicted of launching sophisticated phishing scams to access the accounts of bank customers in 14 countries.

About 2,600 phishing pages that mimicked banking websites were analysed by the Met Police Central e-Crime Unit (PCeU), the Serious Organised Crime Agency and the US Secret Service.

The men behind the scam were traced to the United Kingdom, where they stayed in plush hotels in London while continuing to scam victims.

Officers later discovered servers containing details of 30,000 bank customers, 12,500 of which were in the United Kingdom, and 70 million customer email addresses to be used in phishing scams.

The men were jailed in 2016 for a total of 20 years. Investigating officer DI Jason Tunn said at the time that it was the "biggest case the PCeU has dealt with to date and is likely to be the biggest cyber phishing case so far in the United Kingdom".

It was the United Kingdom's biggest ever cyber fraud. At the height of the scam it raked in up to £2million a week.

Source (with modification): UK's biggest ever cyber scammers stole £113m by calling victims pretending to be from their BANK: Fraudsters used bin bags full of cash for shopping sprees, bought supercars and a Lahore mansion. https://www.dailymail.co.uk/news/article-3792417/Fraud-ring-boss-gang-stole-113million-UK-firms.html

Credential Stuffing

Credential stuffing is a type of cyberattacks where stolen account credentials typically consisting of lists of usernames and/or email addresses and the corresponding passwords (often from a data breach on a third- party server) are used to gain unauthorized access to user accounts through large-scale automated login requests directed against a web application. Credential stuffing attacks are possible because many users reuse the same username/password combination across multiple sites, with one survey reporting that 81 per cent of users have reused a password across two or more sites and 25 per cent of users use the same password across a majority of their accounts.[6]

Case Study 4: United States of America's State Farm accounts compromised in credential stuffing attack

In August 2019, United States of America's insurance company State Farm sent out email notifications to users whose online account login credentials were discovered by an attacker during a credential stuffing attack.

The attacker had compile usernames and passwords that were leaked from other organizations' data breaches and used those credentials to try and gain access to accounts at State Farm. State Farm had also reset the passwords for accounts whose login credentials were discovered by the attacker.

Source (with modification): State Farm Accounts Compromised in Credential Stuffing Attack https://www.bleepingcomputer.com/news/security/state-farm-accounts-compromised-in-credential-stuffing-attack/-113million-UK-firms.html

Malicious code

Malicious code refers to programs that cause damage to a system when executed. Viruses, worms and Trojan horses are types of malicious code.

A computer **virus** is a computer program or programming code that damages computer systems and data by replicating itself by initiating copying to another program, computer boot sector or document.

A **worm** is a self-replicating virus that does not alter files but resides in active memory, using parts of an operating system that are automatic and usually invisible to the user. Their uncontrolled replication consumes system resources, slowing or halting other tasks. It is usually only when this happens that the presence of worms is detected.

[6] Ibid.

A **Trojan horse** is a program that appears to be useful and/or harmless but really has a malicious function such as unloading hidden programs or command scripts that make a system vulnerable to encroachment.

Case Study 5: Islamic Republic of Iran: The Stuxnet worm marks a new era of cyberwar

The Stuxnet worm was discovered on computers in the Islamic Republic of Iran in June 2010 by a Belarusian security firm. The worm had infected more than 100,000 computer systems worldwide, most of them in Iran.

The Los Angeles Times reports that: “Stuxnet is being called the most sophisticated cyber weapon ever unleashed, because of the insidious way in which it is believed to have secretly targeted specific equipment used in Iran’s nuclear program.”

The targeted code was designed to attack Siemens Simatic WinCC SCADA systems. The Siemens system is used in various facilities to manage pipelines, nuclear plants, and various utility and manufacturing equipment. Although the Stuxnet worm affected many systems, it is speculated by many that the worm was created specifically to target Iran’s nuclear facility. The creator of the worm is yet unknown.

Sources (with modification): Ken Dilanian, “Iran’s nuclear program and a new era of cyber war”, *Los Angeles Times*, 17 January 2011, http://articles.latimes.com/2011/jan/17/world/la-fg-iran-cyber-war-20110117;

Kim Zetter, “Iran: Computer Malware Sabotaged Uranium Centrifuges”, Wired, 29 November 2010, http://www.wired.com/threatlevel/2010/11/stuxnet-sabotage-centrifuges/; and Wikipedia, “Stuxnet”, http://en.wikipedia.org/wiki/Stuxnet.

A **Ransomware** is a program that appears to be useful and/or harmless but really has a malicious function such as threatening to publish the victim’s data or perpetually block access to it, unless ransom is paid.

Case Study 6: WannaCry cyber-attack cost the NHS £92m as 19,000 appointments cancelled

The so-called WannaCry hack, which shut down hundreds of thousands of computers around the world with messages from hackers demanding ransom payments, hit a third of hospital trusts and 8pc of GP practices. Around 1pc of all NHS care was disrupted over the course of a week.

The hack caused more than 19,000 appointments to be cancelled, costing the NHS £20m between 12 May and 19 May and £72m in the subsequent cleanup and upgrades to its IT systems

The cyber-attack caused 200,000 computers to lock out users with red-lettered error messages demanding the cryptocurrency Bitcoin. The attack was blamed on elite North Korean hackers after a year-long investigation.

Sources (with modification): The Telegraph; WannaCry cyber-attack cost the NHS £92m as 19,000 appointments cancelled, https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled

Advanced Persistent Threat

An advanced persistent threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization.[7] APT attacks target organizations in sectors with high-value information, such as national defense, manufacturing and the financial industry.

An APT attacker often uses “spear fishing”, a type of social engineering, to gain access to the network through legitimate means. Once access has been achieved, the attacker establishes a “back door”.

The next step is to gather valid user credentials (especially administrative ones) and move laterally across the network, installing more back doors. The back doors allow the attacker to install bogus utilities and create a “ghost infrastructure” for distributing malware that remains hidden in plain sight.

[7] Rosencrance, L. (2020, August 27). *What is advanced persistent threat?* SearchSecurity. https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT.

.

Case Study 7: RSA hit by advanced persistent threat attacks

In March 2011, RSA, the security division of EMC, announced that it had been a target of an attack and that information related to RSA's SecurID two-factor authentication products was stolen by attackers.

Investigations had revealed that the attack was in the category of an APT. APT threats are becoming a significant challenge for all large corporations. To identify APTs, organizations need to deploy technologies that not only identify all potential threats through behavior analysis but are also able to test all suspicious elements in a virtual environment.

Two-factor authentication is a preferred method of providing stronger security than is provided by a username and password alone. One of the most common methods of two- factor authentication is to use a key fob or token that provides a randomized code user must enter in addition to the username and password in order to authenticate and gain access to the site or application.

RSA is a leading provider of two-factor authentication solutions, and its key fobs and tokens are virtually ubiquitous. With millions of customers relying on RSA to provide additional security and protect accounts from unauthorized access, it is troubling that malicious hackers may now possess the keys to circumvent that protection.

RSA assured its clients that the information extracted did not enable a successful direct attack on any of their RSA SecurID customers. However, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack. Lockheed-Martin, a client of RSA, was subsequently hacked, and it is speculated to have been carried out by the same hacker (see case study above).

Sources (with modification) : Tony Bradley, "RSA SecurID Hack Shows Danger of APTs", *PCWorld*, 19 Mach 2011, http://www.pcworld.com/ businesscenter/article/222555/rsa_securid_hack_shows_danger_of_apts.html; and Warwick Ashford, "RSA hit by advanced persistent threat attacks", *Computer Weekly*, 18 March 2011, http://www.computerweekly.com/Articles/2011/ 03/18/245974/ RSA-hit-by-advanced-persistent-threat-attacks.htm.

2.3. Types of Internal Attacks

Disgruntled employees/contractors

Internal attacks are one of the biggest threats facing our data and systems. Rogue employees, especially members of the IT team with knowledge of and access to networks, data centers and admin accounts, can cause serious damage to an organizations network, systems and data.

Lack of employee security awareness

Security awareness training for employees helps to eradicate risky behaviors that could potentially lead to cyber breaches. Training programs could address some of the threats faced by an organization, especially attacks such as phishing emails, ransomware, and social engineering scams via the telephone, text message, or social media channels.

Social engineering

The term “social engineering” refers to a set of techniques used to manipulate people into divulging confidential information. Although it is similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access. In most cases the attacker never comes face-to-face with the victim.

2.4. Trends in Information Security Threats[8]

An important activity in safeguarding information security is security threat trend analysis. This refers to the search for patterns in security threats over time in order to identify the ways in which such patterns change and develop, veer to new directions, or shift. This iterative process of collecting and correlating information and improving incident profiles is done to be able to anticipate likely or possible threats and prepare the appropriate responses to these threats.

Organizations that perform information security threat trend analysis and share security threat trend reports include:

- FireEye (https://www.fireeye.com/current-threats/threat-intelligence- reports.html)
- IBM (https://www.ibm.com/security/data-breach/threat-intelligence /)
- Microsoft (www.microsoft.com/en-us/security/operations/security- intelligence-report)
- Symantec (https://www.symantec.com/security-center/threat-report)
- Verizon (https://enterprise.verizon.com/resources/reports/dbir/)

Trends in information security threats that have been reported are described below.

Automation of attack tools[9]

Intruders now use automated tools that allow them to gather information about thousands of Internet hosts quickly and easily. Networks can be scanned from a remote location and hosts with specific weaknesses identified using these automated tools. The intruders catalogue the information for later use, share or trade it with other intruders, or attack immediately. Some tools (such as Cain & Abel) automate a series of small attacks towards an overall objective. For example, intruders can use a packet sniffer to obtain router or firewall passwords, log in to the firewall to disable filters, and then use a network file service to read data on a server.

Attack tools that are difficult to detect

[8] Shimeall, T. J., & Williams, P. (2002). Models of information security trend analysis. *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Defense and Law Enforcement*. https://doi.org/10.1117/12.479291

.

[9] Carnegie Mellon University. *Software Engineering Institute*. The CERT Division. https://www.sei.cmu.edu/about/divisions/cert/index.cfm.

.

Some attack tools use new attack patterns that are not detected by existing detection tools. For example, anti-forensic techniques are being used to mask or hide the nature of attack tools. Polymorphic tools change the form each time they are used. Some of these tools use common protocols like the hypertext transfer protocol (HTTP), making it difficult to distinguish them from legitimate network traffic.[10] The MSN Messenger worm is a good example of this. A worm in the MSN Messenger Instant-Messaging (IM) client sends to contacts from the infected user's address book a file designed to infect systems, after first issuing a warning that they are about to receive a file. The behavior of a real IM user is mimicked, which is alarming.[11]

Faster discovery of vulnerabilities

Every year the newly discovered vulnerabilities in software products that are reported to the Computer Emergency Response Team Coordination Center (CERT/CC) are more than doubles in number, making it difficult for administrators to keep up to date with patches. Intruders know this and take advantage.[12] Some intruders launch a zero-day (or zero hour) attack, which is a computer threat that exploits computer application vulnerabilities for which there are no patches or protection because they have not yet been discovered by administrators.[13]

Increasing asymmetric threat and convergence of attack methods

An asymmetric threat is a condition in which an attacker has the edge over a defender. The number of asymmetric threats increases with the automation of threat deployment and sophistication of attack tools.

Convergence of attack methods refers to the consolidation of diverse attack methods by attackers to create global networks that support coordinated malicious activity. For example, Zbot, known as Zeus, is a malware package that is readily available for sale and also traded in underground forums. The package contains a builder that can generate a bot executable and Web server files (PHP, images, SQL templates) for use as the command and control server. While Zbot is a generic back door that allows full control by an unauthorized remote user, the primary function of Zbot is financial gain—stealing online credentials such as FTP, e-mail, online banking, and other online passwords.[14]

---

[10] Ramasubramanian, S., Ansari, S., & Purcell, F. (2005). Governing Internet Use: Spam, Cybercrime and e-Commerce. In D. Butt (Ed.), *Internet governance: Asia-Pacific Perspectives* (pp. 89–104). essay, APDIP. https://www.unapcict.org/sites/default/files/2019-01/Internet%20Governance%20-%20Asia-Pacific%20perspectives.pdf.

[11] Kotadia, M. (2005, April 5). *E-mail worm graduates to IM*. ZDNet. https://www.zdnet.com/article/e-mail-worm-graduates-to-im/.

[12] Ramasubramanian, S., Ansari, S., & Purcell, F. (2005). Governing Internet Use: Spam, Cybercrime and e-Commerce. In D. Butt (Ed.), *Internet governance: Asia-Pacific Perspectives* (pp. 89–104). essay, APDIP. https://www.unapcict.org/sites/default/files/2019-01/Internet%20Governance%20-%20Asia-Pacific%20perspectives.pdf.

[13] Wikimedia Foundation. (2020, December 31). *Zero-day (computing)*. Wikipedia. https://en.wikipedia.org/wiki/Zero-day_(computing).

[14] Korolov, M. (2019, June 27). *What is a botnet? When armies of infected IoT devices attack*. CSO Online. https://www.csoonline.com/article/3240364/what-is-a-botnet.html.

Increasing threat from infrastructure attacks

Infrastructure attacks are attacks that broadly affect key components of the Internet. They are a concern because of the number of organizations and users on the Internet and the increasing amount of personal data on the Internet to carry out day-to-day business. Infrastructure attacks result in compromise of sensitive information, spread of misinformation, and significant diversion of resources from other tasks.

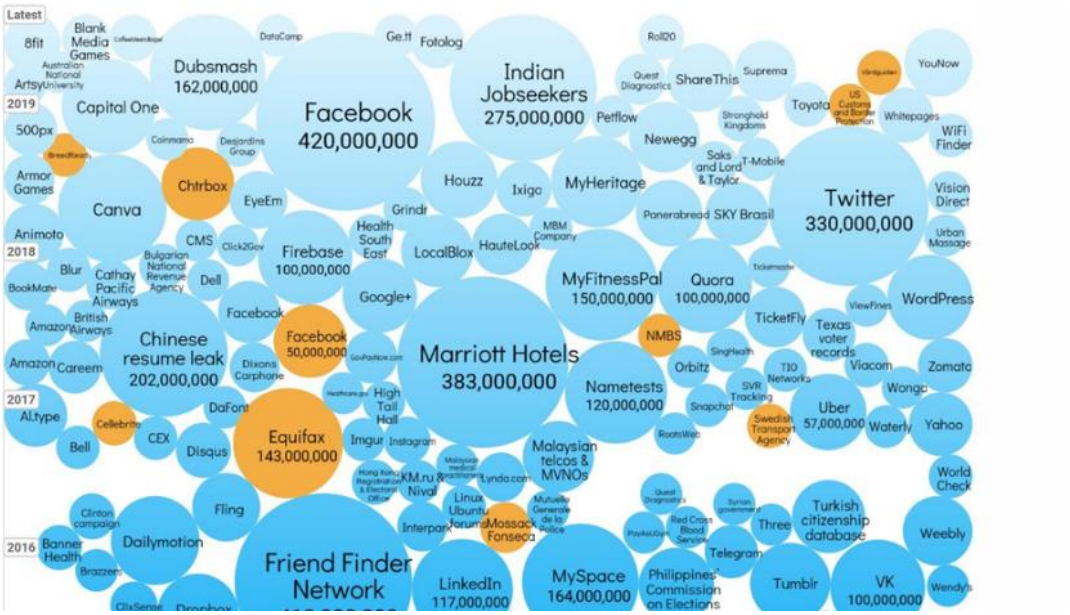
Hacking is an example of an infrastructure attack. The term "hacking" refers to the act of gaining access to a computer or computer network to obtain or modify information without legal authorization.
Hacking can be classified as recreational, criminal or political hacking, depending on the purpose of the attack. Recreational hacking is unauthorized modification of programs and data simply to satisfy the hacker's curiosity. Criminal hacking is used in fraud or espionage. Political hacking is tampering with websites to broadcast unauthorized political messages.[15]

Recently, hacking has become more and more implicated in cyberterror, cyberpolitics and cyberwarfare, posing a major threat to national security.

Another new trend shows hacking groups targeting major sites with national interest and holding highly sensitive information.

Figure 4 shows the trend in data breach volumes.

Figure 4: Data breach statistics



Source: Information is Beautiful.

[15] Denning, D. E., Arquilla, J., & Ronfeldt, D. (2001). Activism, Hacktivism, And Cyberterrorism: The Internet As A Tool For Influencing Foreign Policy. In *Networks and Netwars. The Future of Terror, Crime, and Militancy* (pp. 239–288). essay, RAND Corporation.

Case Study 8: Countering Hacking – A national case study

The Attorney General's Office of the Republic of Indonesia is institutionally strengthening and revitalizing the institution by preparing, designing and formulating Cybercrime Task Force, which will consist of prosecutors who specifically have knowledge, abilities, skills and expertise in handling cybercrime cases.

The Task Force will consist of three special units, namely:

- First, Computer Related Crime Unit, assigned to handle criminal cases that utilize computers or information technology facilities as a means of committing crimes,
- Second, Crimes Against Computer Unit, assigned to handle crimes aimed at computers and information technology; and
- Third, Cooperation and Secretariat Unit, providing support in handling cases and cooperation both nationally and internationally.

Technical: Tools and techniques to identify and gather information about active botnets

- Information security and privacy best practices to mitigate botnet activity
- Registrar and registry best practices to mitigate botnet activity
- Capacity building for e-commerce and online transaction providers

Social: Broad-based education initiatives on Internet safety and security

- Facilitation of secure ICT access for users

The PTF ITU SPAM toolkit is a comprehensive package to help policy planners, regulators and companies adjust policy and recover confidence in e-mail. The toolkit also recommends sharing of information across countries to prevent international problems.

Changes in purpose of attacks

It used to be that computer and network attacks were perpetrated out of curiosity or for self-satisfaction. Now, the purpose is usually money, slander and destruction. Moreover, these types of attacks represent only a small portion of the broad spectrum of cybercrime.

Cybercrime is the deliberate destruction, disruption or distortion of digital data or information flows for political, economic, religious or ideological reasons. The most common crimes include hacking, DoS, malicious code and social engineering. Recently, cybercrime has become part of cyber terrorism and cyberwarfare, with adverse effects on national security.

Table 3 below shows what perpetrators of cybercrime earn.

Table 3: Returns from cybercrime in 2017

Item	Price Ranges (in USD)
General non-financial institution login credentials	1
Credit or Debit Card	5-110
Driver's License, Loyalty accounts	20
Online payment services login info e.g. Paypal	20-200
Diplomas	100-400
Medical Records	1-1,000
Passports	1,000-2,000

Source: Experian

Stack, B. (2017, December 6). *Here's How Much Your Personal Information Is Selling for on the Dark Web*. Experian. https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

2.5 Improving Security

Given the trends in security threats and attack technologies, a robust defense requires a flexible strategy that allows adaptation to the changing environment, well-defined policies and procedures, the use of appropriate security technologies, and constant vigilance.

It is helpful to begin a security improvement programme by determining the current state of security. Integral to a security programme are documented policies and procedures, as well as technology that supports their implementation.

Administrative security

Administrative security consists of an information security strategy, policy and guidelines.

An **information security strategy** sets the direction for all information security activities.

An **information security policy** is a documented high-level plan for organization-wide information security. It provides a framework for making specific decisions, such as an administrative and physical security plan.

Because an information security policy should have a long-term point of view, it should avoid technology-specific content and include effective business continuity planning development.

Information security guidelines should be established according to the information security strategy and policy. The guidelines should specify regulations for each area related to information security. And because the guidelines must be comprehensive and national in scope, they must be developed and delivered by the government for observance by organizations.

Information security standards must be specialized and specific so that they can be applied to all security information areas. It is good for each country to develop standards after analysing the administrative, physical and technical security standards that are widely used all over the world. Standards should be appropriate to the prevailing ICT environment.

A country's information security strategy, policy and guidelines should be in compliance with related law. Their scope should be within the boundaries of national and international laws.

Information security operation and process

Once an information security strategy, policy and guidelines are established, information security operating procedures and processes will need to be defined. Because people are the ones who perpetrate attacks on information or leak internal information, human resources management is the most important factor in operating information security. Hence the need for the following:

1. Information security education and training programme – There are many methods to improve an organization's level of information security, but education and training are the basic activities. The members of an organization must appreciate the need for information security and acquire related skills through education and training. However, it is important to develop various programmes for maximizing participation because standardized information security education and training programmes may not be effective.

2. Strengthening promotion through a variety of events – Employee participation is important in the successful implementation of information security strategy, policy and guidelines. Information security should be promoted among employees through various daily activities.

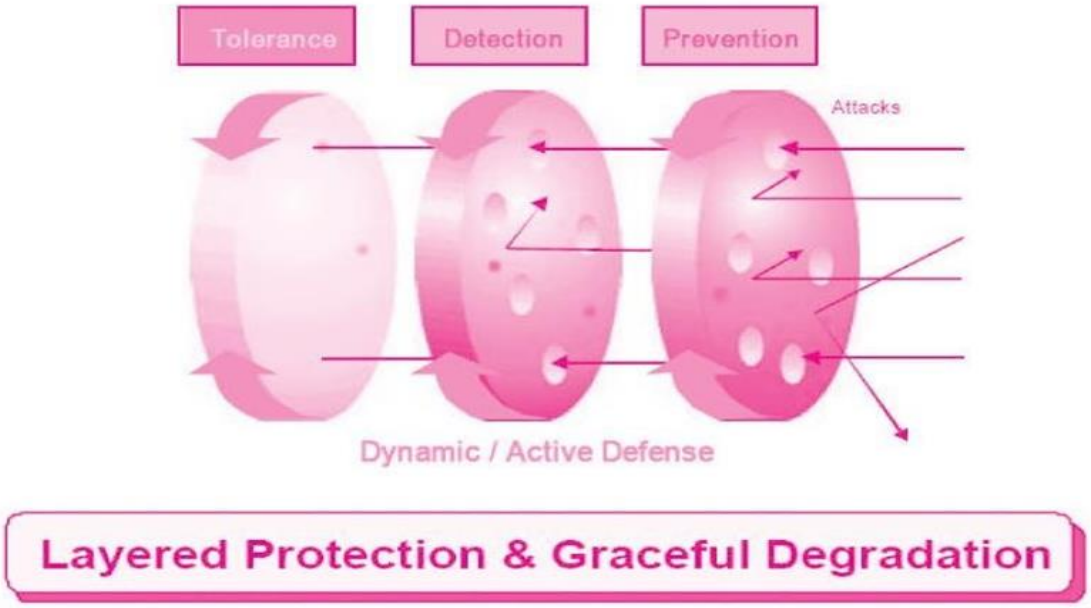
3. Securing sponsorship – While there may be high levels of information security awareness among employees and they have a strong will to maintain information security, it is difficult to ensure information security without support from the highest levels of the organization. The support of the Chief Executive Officer and Chief Information Officer should be obtained.

Technological security

Various technologies have been developed to help organizations secure their information systems against intruders. These technologies help to protect systems and information against attacks, to detect unusual or suspicious activities, and to respond to events that affect security.

Today's security systems have been designed and developed based on a Defense-In-Depth (DID) model that leads to unified management of the technologies involved. This model is different from perimeter defence, which has only one layer of defence against all threats. The DID model consists of prevention, detection and tolerance, with threats being reduced at each phase (see figure 5).

Figure 5: Defense-In-Depth model



Source: Defense Science Board Task Force, *Protecting the Homeland: Defensive Information Operations 2000 Summer Study Volume II* (Washington, D.C., 2001), p. 5, http://www.carlisle.army.mil/DIME/documents/dio.pdf.

Prevention technology

Prevention technologies protect against intruders and threats at the storage or system level. These technologies include the following:

1. Cryptography – Also referred to as encryption, cryptography is a process of translating information from its original form (called plaintext) into an encoded, incomprehensible form (called ciphertext). Decryption refers to the process of taking ciphertext and translating it back into plaintext. Cryptography is used to protect various applications. More information about cryptography and related technologies (IPSec, SSH, SSL, VPN, OTP, etc.) is available at the following Web pages:

    - IETF RFC (http://www.ietf.org/rfc.html)
    - RSA Laboratories' Frequently Asked Questions About Today's Cryptography (http://www.rsa.com/rsalabs/node.asp?id=2152)

2. One-time passwords (OTPs) – As the name implies, OTPs can be used only once. Static passwords can more easily be accessed by password loss, password sniffing, brute-force password cracks, and the like. This risk can be greatly reduced by constantly altering a password, as is done with an OTP. For this reason, OTP is used to secure electronic financial transactions such as online banking.

3. Firewalls – Firewalls regulate some of the flow of traffic between computer networks of different trust levels such as between the Internet, which is a no-trust zone, and an internal network, which is a zone of higher trust. A zone with an intermediate trust level, situated between the Internet and a trusted internal network, is often referred to as a "perimeter

network” or demilitarized zone.

4. Vulnerability analysis tool – Because of the increase in the number of attack methods and the vulnerabilities present in commonly used applications, it is necessary to periodically assess a system’s vulnerabilities. In computer security, a vulnerability is a weakness that allows an attacker to violate a system. Vulnerabilities may result from weak passwords, software bugs, a computer virus, a script code injection, an SQL injection or malware. Vulnerability analysis tools detect these vulnerabilities. They are easily available online and there are companies that provide analytic services. However, those that are freely available to the Internet community could be misused by intruders. For more information, see:

   - Secunia Vulnerability Research (https://www.flexera.com/products/operations/software-vulnerability-research/secunia-research/advisories.html)
   - SecurityFocus Vulnerability Archive (http://www.securityfocus.com/bid)
   - Top 100 Network Security Tools (http://sectools.org)

   Network vulnerability analysis tools analyse vulnerabilities of network resources such as routers, firewalls and servers.

   A server vulnerability analysis tool analyses such vulnerabilities as a weak password, weak configuration and file permission error in the internal system. A server vulnerability analysis tool provides relatively more accurate results than does a network vulnerability analysis tool because this tool analyses many more vulnerabilities in the internal system.

   Web vulnerability analysis tools analyse vulnerabilities of Web applications such as XSS and SQL Injection throw web. For more information, see the Open Web Application Security Project at https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

5. Air Gap tool – An air gap, air wall or air gapping is a network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network. For years, the prevailing advice from most cybersecurity experts has been to approach security with a defense-in-depth strategy (i.e., multiple layers of protection) rather than with an air gap strategy.

6. Browser isolation – This is a cybersecurity model which aims to physically isolate an internet user's browsing activity (and the associated cyber risks) away from their local networks and infrastructure. Browser isolation technologies approach this model in different ways, but they all seek to achieve the same goal, effective isolation of the web browser and a user's browsing activity as a method of securing web browsers from browser-based security exploits, as well as web-borne threats such as ransomware and other malware.

Detection technology

Detection technology is used to detect and trace abnormal states and intrusion in networks or important systems. Detection technology includes the following:

1. Antivirus – An antivirus software is a computer program for identifying, neutralizing or eliminating malicious code, including worms, phishing attacks, rootkits, Trojan horses and other malware.[16]

2. Intrusion detection system (IDS) – An IDS gathers and analyses information from various areas within a computer or a network to identify possible security breaches. Intrusion detection functions include analysis of abnormal activity patterns and ability to recognize attack patterns.

3. Intrusion prevention system (IPS) – Intrusion prevention attempts to identify potential threats and respond to them before they are used in attacks. An IPS monitors network traffic and takes immediate action against potential threats according to a set of rules established by the network administrator. For example, an IPS might block traffic from a suspicious IP address.[17]

4. Malware sand box system – A "malware sandbox" is a security system that separates execution of programs, usually in an effort to mitigate malware from spreading. It is often used to execute untested or untrusted programs or code, possibly from unverified or untrusted third parties, suppliers, users or websites, in a “sandbox” without risking harm to the host machine or operating system. The sandbox typically tightly controls the programs, and restricts the program’s access to disk, memory and network.

5. Network Traffic Analysis (NTA) – Network traffic analysis is an active cyber defence activity. It is "the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions”[18]. This is in contrast to traditional threat management measures, such as firewalls, intrusion prevention systems (IDS) and malware sandbox systems, which typically involve an investigation of evidence-based data after there has been a warning of a potential threat.

Integration technology

Integration technology integrates important functions for the information security of core assets, such as predicting, detecting and tracing intrusions. Integration technology includes the following:

---

[16] Wikimedia Foundation. (2021, February 1). *Antivirus software*. Wikipedia. http://en.wikipedia.org/wiki/Antivirus_software.

[17] Gillis, A. S. (2020, February 12). *What is an Intrusion Prevention System (IPS)?* SearchSecurity. https://searchsecurity.techtarget.com/definition/intrusion-prevention.

[18] Egede, I. (2018, July 31). Threat Hunting for File Hashes as an IOC. Infosec Resources. https://resources.infosecinstitute.com/topic/threat-hunting-for-file-hashes-as-an-ioc.

1. Enterprise security management (ESM) – An ESM system manages, controls and operates an information security solution such as an IDS and IPS based on a consistent policy. It is used as a strategy to make up for the weakness of other solutions by using the advantages of each information security solution and maximizing the efficiency of information security under a consistent policy.

   ESMs that can manage existing security technologies synthetically came about recently due to the shortage of human resources operating security technologies, the increase in upgraded attacks such as convergence of attack methods, and the emergence of attack tools that are difficult to detect. With ESM, the efficiency of management is raised and active countermeasures are established.

2. Enterprise risk management (ERM) – ERM is a system that helps to predict all risks related to organizations, including in areas outside of information security, and automatically configure countermeasures. Use of ERM to protect information requires that the exact purpose of risk management and design for the development of the system are specified. Most organizations construct and optimize their own ERMs through professional information security consulting agencies instead of doing it by themselves.

Questions to Think About

1. What information security threats is your organization vulnerable to? Why?

2. Which information security technology solutions are available in your organization?

3. Does your organization have an information security policy, strategy and guidelines? If yes, how adequate are these given the threats that your organization is vulnerable to? If none, what would you recommend by way of an information security policy, strategy and guidelines for your organization?

Test Yourself

1. Why is it important to conduct information security threat trend analysis?

2. Why is human resources management the most important factor in information security operations? What are the key activities in human resources management for information security?

3. Explain the Defense-In-Depth model of technology security. How does it work?

3. Information Security Activities

This section aims to:

Give examples of information security activities of various countries to serve as a guide in information security policymaking; and

Highlight international cooperation in implementing information security policy

3.1. Development of National Information Security Strategy

Information security strategy

The need for the National Information Security Strategy (NISS) is dictated by the complexity of today's interconnected computer networks. Government agencies need to be responsible for the security of their information and Information Communications Technology (ICT) systems. In fact, national agencies are increasingly reliant on also third-party ICT systems operated by commercial entities that may extend beyond their national borders.

While most countries recognize the need to better align information security with the goals of their nations, many are still struggling to translate this recognition into concrete plans of action.

It is common in the development of a NISS to state its vision. Some common objectives include

- A Secure, Reliable and Resilient National ICT Infrastructure Environment
- A Highly Skilled Cyber Security Workforce
- A National Cyber Security Awareness and Training Program
- Enactment of National Legislation to Address Cyber Crime
- National and International Security Cooperation

In more advanced NISS strategies, objectives such as the following are also included

- A National Cyber Threat Analysis and Response Program
- A National Cyber Security Compliance and Tracking Program
- A National Cyber Security Research, Innovation and Entrepreneurship Program

In the development of the NISS, it is common to either adopt international standards or codes of practice.

Examples of technical standards include ISO 27001 and UN/EDIFACT (United Nations/Electronic Data Interchange for Administration, Commerce and Transport).

Examples of Code of Conduct include the Council of Europe and OECD.

Examples of Industry Practices and Requirements include the European Security Forum (ESF), National Institute of Standards and Technology (NIST) and the United Kingdom's Department of Trade and Industry (DTI).

3.2. Examples of National Information Security Strategies

Information security strategy of the United States of America

After the terrorist attacks on 11 September 2001 (9/11), the Government of the United States of America established the Department of Homeland Security to strengthen national security not only against physical threats but also against cyberthreats.

The United States of America's information security strategy includes the National Strategy for Homeland Security, National Strategy for the Physical Security of Critical Infrastructures and Key Assets, and National Strategy to Secure Cyberspace.

The National Strategy to Secure Cyberspace[19] sets the vision of cybersecurity and protection of critical infrastructure and assets. It defines the specific goals and activities for preventing cyberattacks against critical infrastructure and assets. The five national priorities defined in the National Strategy to Secure Cyberspace are:

- A National Cyberspace Security Response System
- A National Cyberspace Security Threat and Vulnerability Reduction Program
- A National Cyberspace Security Awareness and Training Program
- Securing Government's Cyberspace
- National Security and International Cyberspace Security Cooperation

The latest National Cyber Strategy[20] was released on September 2018. The four key pillars defined are:

- Protect the American People, the Homeland, and the American Way of Life
  - Secure Federal Networks and Information
  - Secure Critical Infrastructure
  - Combat Cybercrime and Improve Incident Reporting
- Promote American Prosperity
  - Foster a Vibrant and Resilient Digital Economy
  - Foster and Protect United States of America's Ingenuity
  - Develop a Superior Cybersecurity Workforce
- Preserve Peace through strength
  - Enhance Cyber Stability through Norms of Responsible State Behavior

[19] The White House. (2003). (rep.). *The National Strategy to Secure Cyberspace*. Retrieved from https://www.hsdl.org/?view&did=1040

[20] The White House. (2018). (rep.). *National Cyber Strategy of the United States of America*. Retrieved from https://www.defense.gov/Explore/News/Article/Article/1641969/white-house-releases-first-national-cyber-strategy-in-15-years/

- Attribute and Deter Unacceptable Behavior in Cyberspace
- Advance American Influence
  - Promote an Open, Interoperable, Reliable and Secure Internet
  - Build International Cyber Capacity

Tightening up information security law

The **Cyber Security Enhancement Act of 2014** (CSEA)[21] was first enacted in 2002 and the latest revision in 2014. It comprises the second chapter of the Homeland Security Law. It provides for amendments to sentencing guidelines for certain computer crimes, emergency disclosure exception, good faith exception, prohibition of illegal Internet advertisement and protection of privacy, among others. The bill also provides for "an ongoing, voluntary public-private partnership to improve cybersecurity, and to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness, and for other purposes."

Information security strategy of the United Kingdom

The United Kingdom government released latest National Cyber Security Strategy 2016-2021[22]. The vision of 2021 is that the United Kingdom is secure and resilient to cyber threats, prosperous and confident in the digital work.

(https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf)

To realize this vision, it states the following objectives

- Defend
  - We have the means to defend the United Kingdom against evolving cyber threats, to respond effectively to incidents and to ensuring the United Kingdom networks, data and systems are protected and resilient

- Deter
  - The United Kingdom will be a hard target for all forms of aggression in cyberspace. We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should be choose to.

- Develop

[21] U.S. Government Printing Office. (2014). *An Act to Provide for an Ongoing, Voluntary Public-Private Partnership to Improve Cybersecurity, and to Strengthen Cybersecurity Research and Development, Workforce Development and Education, and Public Awareness and Preparedness, and for Other Purposes*.

[22] HM Government. (2016). (rep.). *National Cyber Security Strategy 2016-2021*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

- We have an innovative, growing cyber security industry, underpinned by world-leading scientific research and development. We have a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors. Our cutting-edge analysis and expertise will enable the United Kingdom to meet and overcome future threats and challenges.

Information security strategy of the European Union

Currently, countries in the European Union have a National Cybersecurity Strategy (NCSS) as a key policy feature, helping them to tackle risks which have the potential to undermine the achievement of economic and social benefits from cyberspace.

In a Communication dated May 2006[23], the European Commission describes the recent European Union (EU) strategy for information security as consisting of a number of interdependent measures involving many stakeholders. These measures include the establishment of a Regulatory Framework for Electronic Communications in 2002, the articulation of the i2010 initiative for the creation of a European Information Society, and the setting up of the European Network and Information Security Agency (ENISA) in 2004. According to the Communication, these measures reflect a three-pronged approach to security issues in the Information Society embracing specific network and information security (NIS) measures, the regulatory framework for electronic communications (which includes privacy and data security issues), and the fight against cybercrime.

In a Communication dated December 2006, the European Commission launched the European Programme for Critical Infrastructure Protection (EPCIP) to reduce the vulnerabilities of critical infrastructures.[24] This is a package of measures aimed at improving the protection of critical infrastructure in Europe, across all European Union States and in all relevant sectors of economic activity. The European Union initiative on Critical Information Infrastructure Protection (CIIP) aims to strengthen the security and resilience of vital Information and Communication Technology (ICT) infrastructures.

(https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF)

The Communication notes attacks on information systems, increasing deployment of mobile devices, the advent of “ambient intelligence”, and improving the awareness level of users as the main security issues that the European Commission aims to address through dialogue, partnership and empowerment. These strategies are described in the Communication (see box 2).

[23] Commission of the European Communities, A strategy for a Secure Information Society – “Dialogue, partnership and empowerment” (2006). Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0251&qid=1612332935197&from=EN.

[24] Commission of the European Communities, A European Programme for Critical Infrastructure Protection (2006). Brussels, Belgium. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.

Box 2: European Commission's multi-stakeholder dialogue

The Commission proposes a series of measures designed to establish an open, inclusive and multi-stakeholder dialogue:

- A benchmarking exercise for national policies relating to network and information security, to help identify the most effective practices so that they can then be deployed on a broader basis throughout the EU. In particular, this exercise will identify best practices to improve the awareness of small and medium enterprises (SMEs) and citizens of the risks and challenges associated with network and information security; and
- A structured multi-stakeholder debate on how best to exploit existing regulatory instruments. This debate will be organized within the context of conferences and seminars.

Partnership

Effective policymaking requires a clear understanding of the nature of the challenges to be tackled, as well as reliable, up-to-date statistical and economic data. Accordingly, the Commission will ask ENISA to:

- Build a partnership of trust with member States and stakeholders in order to develop an appropriate framework for collecting data; and
- Examine the feasibility of a European information sharing and alert system to facilitate effective response to threats. This system would include a multilingual European portal to provide tailored information on threats, risks and alerts.

In parallel, the Commission will invite member States, the private sector and the research community to establish a partnership to ensure the availability of data pertaining to the ICT security industry.

In March 2009, the Commission adopted a Communication on Critical Information Infrastructure Protection (CIIP) – "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience".[25] It sets out a plan (the "CIIP action plan") to strengthen the security and resilience of vital ICT infrastructures. The aim was to stimulate and support the development of a high level of preparedness, security and resilience capabilities both at national and European levels. This approach was broadly endorsed by the Council in 2009.[26] The CIIP action plan is built on five pillars: (1) preparedness and prevention; (2) detection and response; (3) mitigation and recovery; (4) international cooperation; and (5)

[25] Commission of the European Communities, Critical Information Infrastructure Protection: "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (2009). Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009DC0149&qid=1612333230526&from=EN.

[26] Council of the European Union, Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security (2009). Belgium, Brussels. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF.

criteria for the European Critical Infrastructures in the field of ICT. The CIIP action plan sets out the work to be done under each pillar by the Commission, the member States and/or industry, with the support of ENISA.

The Digital Agenda for Europe (DAE)[27] adopted in May 2010, and the related Council Conclusions[28] highlighted the shared understanding that trust and security are fundamental pre-conditions for the wide uptake of ICT and therefore for achieving the objectives of the "smart growth" dimension of the Europe 2020 Strategy.[29] The DAE emphasizes the need for all stakeholders to join forces in a holistic effort to ensure the security and resilience of ICT infrastructures. To achieve this, the DAE stressed the need to focus on prevention, preparedness and awareness, as well as develop effective and coordinated mechanisms to respond to new and increasingly sophisticated forms of cyberattacks and cybercrime. This approach ensures that both the preventive and the reactive dimensions of the challenge are duly taken into account.

The following measures, announced in the Digital Agenda, have been taken:

- The Commission adopted in September 2010 a proposal for a Directive on attacks against information systems.[30] It aims to strengthen the fight against cybercrime by approximating member States' criminal law systems and improving cooperation between judicial and other competent authorities. It also introduces provisions to deal with new forms of cyberattacks, in particular botnets.

- Complementing this, the Commission at the same time tabled a proposal[31] for a new mandate to strengthen and modernize ENISA in order to boost trust and network security. Strengthening and modernizing ENISA will help the European Union, member States and private stakeholders develop their capabilities and preparedness to prevent, detect and respond to cybersecurity challenges.

Council of Europe Convention on Cybercrime

[27] European Commission, A Digital Agenda for Europe (2010). Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245&qid=1612333676302&from=EN.

[28] Council of the European Union, Council Conclusions on the Digital Agenda for Europe (2010). Brussels, Belgium. https://data.consilium.europa.eu/doc/document/ST-10130-2010-INIT/en/pdf.

[29] European Council, Conclusions of the European Council (25/26 March 2010) (2010). Brussels, Belgium. https://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ec/113591.pdf.

[30] European Commission, Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision (2010). Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010PC0517&qid=1612334410667&from=EN.

[31] European Commission, Proposal For A Regulation Of The European Parliament And Of The Council Concerning The European Network And Information Security Agency (ENISA) (2010). Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010PC0521&qid=1612334562226&from=EN.

In 2001, the European Union promulgated the Council of Europe Convention on Cybercrime (CECC) that “lays down guidelines for all governments wishing to develop legislation against cybercrime” and “provides a framework for international co-operation in this field.” 39 European countries signed the treaty, as well as Canada, Japan, South Africa and the United States of America. This makes the CECC, which entered into force in July 2004, “the only binding international treaty on the subject to have been effectuated to date.”[32]

European Network and Information Security Agency (ENISA)

ENISA was established by the European Parliament and European Union Council on 10 March 2004 “to help increase network and information security within the [European Union] Community and to promote the emergence of a culture of network and information security for the benefit of citizens, consumers, businesses and public sector organizations.”[33]

The Permanent Stakeholders Group (PSG) Vision for ENISA[34] articulated in May 2006 sees ENISA as a center of excellence in network and information security, a forum for NIS stakeholders, and a driver of information security awareness for all European Union citizens. To this end, the following long-term actions for ENISA are stipulated in the PSG Vision (see figure 6):

Figure 6: Long-term action for ENISA

Source: Permanent Stakeholders' Group. (P. Dorey & S. Perry, Eds.), The PSG Vision for ENISA (2006). https://www.enisa.europa. eu/about-enisa/structure-organization/psg/files/psg-vision.

[32] *Council of Europe action against Cybercrime*. Council of Europe. https://www.coe.int/en/web/portal/coe-action-against-cybercrime.

[33] European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration (2010). Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010PC0520&qid=1612335155929&from=EN.

[34] Permanent Stakeholders' Group. (P. Dorey & S. Perry, Eds.), The PSG Vision for ENISA (2006). https://www.enisa.europa. eu/about-enisa/structure-organization/psg/files/psg-vision.
.

1. **Cooperate and coordinate member States' national network and information security authorities**

Cooperation between national agencies is very low at the moment. Much good can be done by fostering increasing communication and cooperation between the national agencies, particularly in sharing best practice from advanced agencies to those who are just starting.

2. **Cooperate with research institutes**

ENISA's purpose should be to direct basic research and targeted technical development in order to focus on the areas of greatest benefit to managing actual security risk in real-world systems. ENISA should not support a research agenda by itself, but rather work on aligning existing processes and priorities of existing programmes.

3. **Cooperate with software and hardware vendors**

Vendors of software and hardware are by definition competitors and it can be difficult for them to openly agree on mutual practices. ENISA could provide unbiased opinion and a forum for sensitive discussions, while maintaining the necessary hygiene against anti-competitive behavior.

ENISA's long-term vision should focus more on creating reliable network and information technologies that are resistant to worms and other problems, instead of extending current incremental security trends. This could be achieved with the promotion of techniques for developing correct, secure and reliable architectures and software.

4. **Participate in standard-setting bodies**

With an eye to identifying and publicizing initiatives of greatest value, ENISA should track and monitor NIS-related topics in standards-setting bodies, including following up the work of various available security certification and accreditation bodies.

5. **Participate in legislative process through lobbying and opinions**

ENISA should work to gain the position of a trusted consultant body to be heard early in the process of drafting and proposing directives and other legislation in NIS-related issues.

6. **Work with user organizations**

Often user organizations are not as well represented in legislative and standard-setting bodies as are vendors. ENISA could provide end user groups with an insight into standards work and an opportunity to influence such work.

7. Identify and promote best practices of member States to end user industry

ENISA should not only protect business interests, but also enhance end users' confidence in the use of the Internet and digital media.

8. Work for a technical and political solution for identity management

Lack of confidence in the Internet is the main obstacle to large-scale consumer-oriented e-business. Being able to accurately check the identity of an owner of a site, an e-mail address, or some online service would be a huge step to renew and increase the common user's trust in the Internet. Technical solutions in this area should be sought through industry-led processes, but ENISA could work towards European Union-wide policies for authentication of online entities.

9. Balance the efforts for both "information" and "network" security issues

ENISA should communicate with the largest Internet and network service providers (ISPs/ NSPs) to help them identify best practices for the benefit of businesses and consumers across Europe. This is important because ISPs/NSPs can play a key role in improving security in the Internet at large. Sufficient co-operation and coordination of the actions ISPs are taking is lacking at the moment.

Source: Abridged from
Permanent Stakeholders' Group. (P. Dorey & S. Perry, Eds.), The PSG Vision for ENISA (2006). https://www.enisa.europa. eu/about-enisa/structure-organization/psg/files/psg-vision.

ENISA is as a body of expertise, set up by the European Union to carry out very specific technical, scientific tasks in the field of information security, working as a "European Community Agency". The Agency also assists the European Commission in the technical preparatory work for updating and developing Community legislation in the field of NIS.

The main tasks of ENISA focus on:

- Advising and assisting the Commission and the member States on information security and in their dialogue with industry to address security-related problems in hardware and software products;
- Collecting and analyzing data on security incidents in Europe and emerging risks;
- Promoting risk assessment and risk management methods to enhance the capability to deal with information security threats; and
- Awareness-raising and cooperation between different actors in the information security field, notably by developing public-private partnerships with industry in this field.

Information security strategy of the Republic of Korea

The Korean government established a comprehensive strategy entitled the “Basic Strategy for Ubiquitous Information Security” in December 2006. The main aims of the strategy are to ensure that Koreans can safely use ICT services in all areas, including financial, educational and medical services; and that personal privacy is protected, and a good information-use environment is implemented. The Basic Strategy for Ubiquitous Information Security expands the concept of information protection to encompass u-Security, u-Privacy, u-Trust and u-Clean.

In the mid-1980s, the Republic of Korea pursued a national informatization plan, but information security as a national goal was a comparably new focus that began in the mid-2000. Studies at that time revealed that the ICT system/financial scales, and the relevant infrastructure and research and development efforts were all very weak. Thus, the Korean government decided to establish key ICT infrastructure in a step-by-step manner through the pursuit of a comprehensive plan. In July 2008, the government launched the Mid-Term Comprehensive Plan for Information Security. This Plan is comprised of six agendas as follows:

1. Improve the nation’s capability in handling cyberattacks
2. Strengthen the protection of national critical information infrastructures
3. Strengthen the personal information protection system
4. Expand information security infrastructures
5. Enhance the competitiveness of the information security industry
6. Establish an information security culture

In April 2019, the National Security Office published the National Cybersecurity Strategy which provides six strategic tasks that are broken down further into 18 main tasks and 73 detailed tasks. Under this plan, the government spelled out its goal of establishing a safe and trustworthy ubiquitous society by ensuring the reliability of the e-government services, eliminating the anxieties of citizens and achieving integrity in business activities.

The six strategic tasks and 18 main tasks are as follows:

1. Increase the Safety of National Core Infrastructure
    a. Strengthen security of national information and communications networks
    b. Improve cybersecurity environment for critical infrastructure
    c. Develop next-generation cybersecurity infrastructure

2. Enhance Cyber Attack Response Capabilities
    a. Ensure cyber-attack deterrence
    b. Strengthen readiness against massive cyber attacks
    c. Device comprehensive and active countermeasures for cyber attacks
    d. Enhance cybercrime response capabilities

3. Establish Governance Based on Trust and Cooperation
    a. Facilitate the public-private military cooperation system
    b. Build and facilitate a nation-wide information sharing system
    c. Strengthen the legal basis for cybersecurity

4. Build Foundations for Cybersecurity Industry Growth
    a. Expand cyber security investment
    b. Strengthen the competitiveness of the cybersecurity workforce and technology
    c. Foster a growth environment for cybersecurity companies
    d. Establish a principle of fair competition in the cybersecurity market

5. Foster a Cybersecurity Culture
    a. Raise cybersecurity awareness and strengthen cybersecurity practice
    b. Balance fundamental rights with cybersecurity

6. Lead International Cooperation in Cybersecurity
    a. Enrich bilateral and multilateral cooperation systems
    b. Secure leadership in international cooperation

The Government of the Republic of Korea believes that Cybersecurity requires participation of not only the government but also individuals and businesses, and the government will strengthen cooperation and open doors to that end, and enhance policy transparency with the ultimate goal of continuously implementing cybersecurity policies based on the public trust.

Information security strategy of Japan[35]

Japan's current cyber security strategy was issued in July 2018. The Cybersecurity Strategic Headquarters was established in November 2014 for the purpose of effectively and comprehensively promoting cyber security policies and headed by the Chief Cabinet Secretary. The National Information Security Center (NISC) which was formed sine 2005 was transformed into the National Centre for Incident readiness and Strategy for Cybersecurity (NISC) an acts as the secretariat of the Cybersecurity Strategy Headquarters in collaboration with the public and private sectors on a variety of activities to create a "free, fair and secure cyberspace". The NISC is the core organization overseeing all information security-related work in Japan.

NISC takes a role of a governmental CERT and NISC and JPCERT/CC, as a CERT covering private entities, work together as a national CERT. NISC comprises of seven groups. Each is required to establish its own roles and plans and operate them (see table 4).

Table 4: Roles and the Group responsible based on the National Strategy on Cybersecurity

Roles	Group
Formulation of medium-to-long term plan on cybersecurity policy and conducting research and analysis of cybersecurity technology trends, etc	Strategy and Policy Planning

[35] *Commitment to a Free,Fair and Secure Cyberspace.* NISC. (2018). https://www.nisc.go.jp/eng/.

Promotion of international cooperation on cyber security policy	International Strategy
Formulation and operation of unified standards for promoting information security measures of government agencies which is a basis of audit	Comprehensive Measures for Government Agencies
Collection of the latest information on cyberattacks and operation of the Government Security Operation Coordination team (GSOC)	Integration and Coordination of Cybersecurity Information
Creation of public-private partnership in cybersecurity measures based on the Cybersecurity Policy for Critical Infrastructure Protection	Critical Infrastructure Protection
Analysis of targeted e-mails and malware, and investigation of other cyberattack cases	Incident Investigation and Analysis
Promotion of cybersecurity measures for the Tokyo Olympic and Paralympic Games 2020	Tokyo 2020

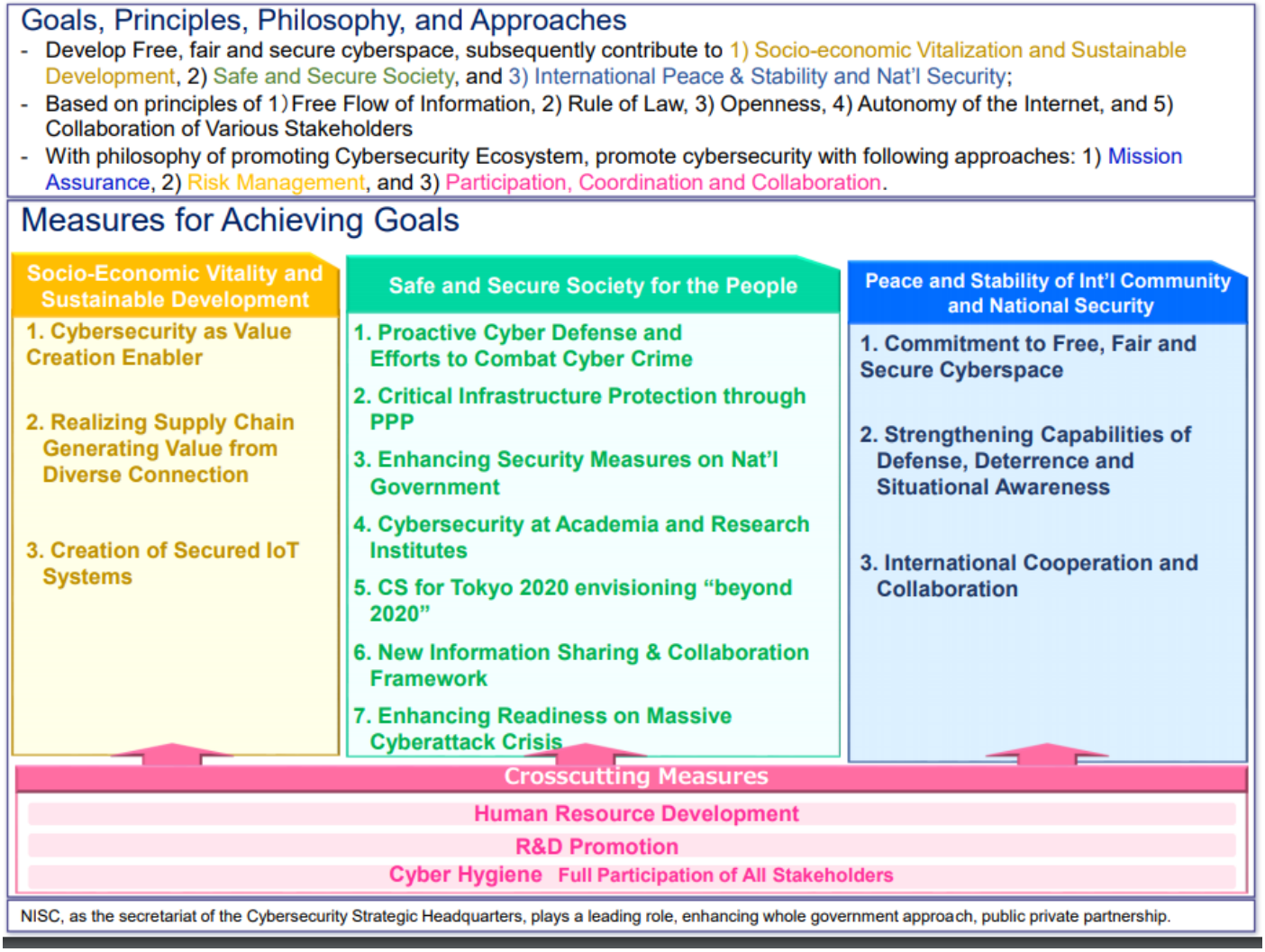
Source (with modification): NISC, http://www.nisc.go.jp/eng/.

The current Cybersecurity Strategy was issued in July 2018 is the second one under the Basic Act on Cybersecurity. The Basic Act on Cybersecurity has been implemented since 2015 to promote the cybersecurity policy by:

- Setting basic principles of cybersecurity policy;
- Clarifying the responsibilities of the government, private entities, and citizens; and
- Stipulating the framework for cybersecurity policy such as the cybersecurity strategy formulation and the establishment of the Cybersecurity Strategic Headquarters

Overview of the current Cybersecurity Strategy is as below (see figure 7 for a summary of the strategy).

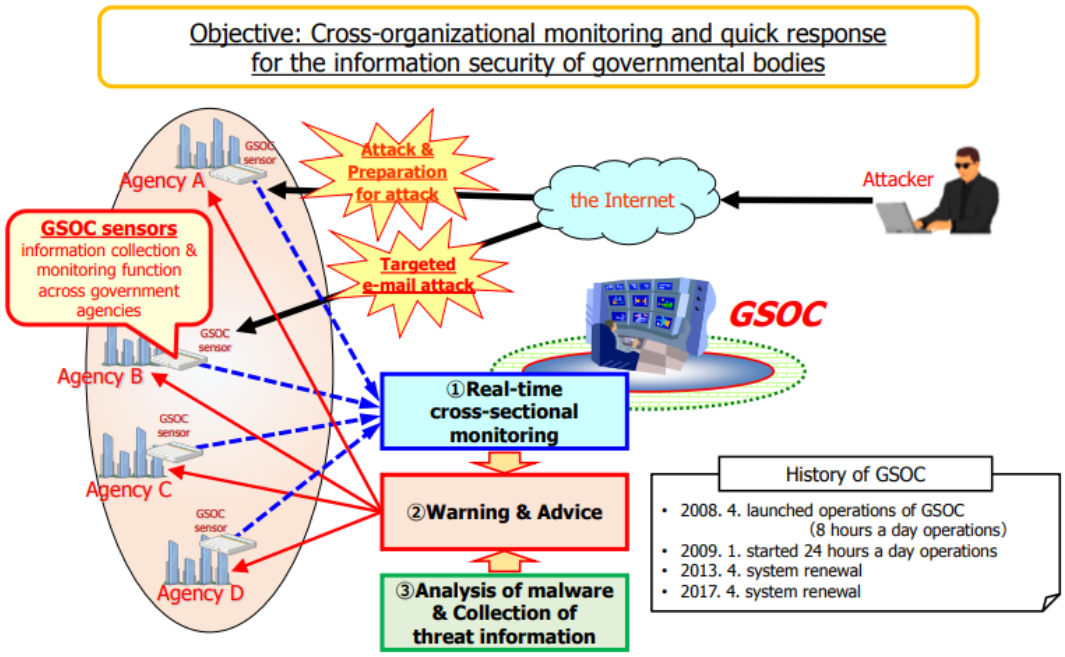
Figure 7: Outline of the National Cybersecurity Strategy



Government Network

NISC operates real-time government-wide monitoring team called the Government Security Operation Coordination team (GSOC). GSOC not only monitors malicious communications incoming to or outgoing from government owned systems but also works as information sharing framework among governmental entities. GSOC provides alerts and advice for the governmental entities when they detect suspicious signals or malware.

Figure 8: Government Security Operation Coordination team (GSOC)



Critical Infrastructure

Since 2005, the 'Cybersecurity Policy for Critical Infrastructure Protection' has been set as a common action plan shared by the government which bears a responsibility for protection of critical infrastructure and by critical infrastructure operators which independently carry out relevant protective measures, and the 4th edition was published in 2017.

This document identifies the 14 sectors as critical infrastructure and it expects stakeholders to undertake the five measures as below.

- Development and penetration of safety principles
- Enhancement of information sharing system
- Reinforcement of incident response capacity
- Risk management and preparation of incident readiness
- Building up of basis of critical infrastructure protection

Questions to Think About

1. How different are the information security activities in your country from those described above?

2. Are there information security activities being undertaken in the countries mentioned in this section that would not be applicable in or relevant to your country? If so, which ones and why would they not be applicable or relevant?

3.3. International Information Security Activities

Information security activities of the United Nations

At the UN-sponsored **World Summit on the Information Society (WSIS)**[36] a declaration of principles and plan of action for effective growth of information society and closing the "information divide" were adopted. The plan of action identifies the following action lines:

- The role of governments and all stakeholders in the promotion of ICTs for development
- Information and communication infrastructure as an essential foundation for an inclusive information society
- Access to information and knowledge
- Capacity building
- Building confidence and security in the use of ICTs
- Creating an enabling environment
- ICT applications in all aspects of life
- Cultural diversity and identity, linguistic diversity and local content
- Media
- Ethical dimensions of the Information Society
- International and regional cooperation[37]

The **Internet Governance Forum (IGF)**[38] is the supporting organization of the United Nations for Internet Governance issues. It was established following the second phase of WSIS in Tunis to define and address issues related to Internet governance. The second IGF forum, held in Rio de Janeiro on 12-15 November 2007, focused on information security issues such as cyberterrorism, cybercrime and the safety of children on the Internet.

Information security activities of the OECD[39]

The Organisation for Economic Co-operation and Development (OECD) is a unique forum where governments of 30 market democracies work together with business and civil society to address the economic, social, environmental and governance challenges facing the globalizing world economy. Within the OECD, the Working Party on Information Security and Privacy (WPISP) works under the auspices of the Committee for Information, Computer and Communications Policy to provide analyses of the impact of ICT on information security and privacy, and to develop policy recommendations by consensus to sustain trust in the Internet economy.

---

[36] International Telecommunications Union. (2006). World Summit on the Information Society : About WSIS. http://www.itu.int/wsis/basic/about.html.

[37] WSIS, WSIS: Plan of Action (2003). International Telecommunications Union. https://www.itu.int/net/wsis/docs/geneva/official/poa.html.

[38] Internet Governance Forum. (2021). http://www.intgovforum.org/.

[39] OECD. (2006, May). OECD Working Party on Information Security and Privacy WPISP. Paris. https://www.gpdp.it/documents/10160/10704/Working+Party+on+Information+Security+and+Privacy.pdf/586b9ff2-0ae8-4cb1-873a-2025fb6f5a15?version=1.1

WPISP work on information security: In 2002, the OECD issued the "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security"[40] to promote "security in the development of information systems and networks and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks."[41]

To share experiences and best practices in information security, the Global Forum on Information Systems and Network Security was held in 2003 and the OECD-APEC Workshop on Security of Information Systems and Networks in 2005.

A project to research methods on countering botnet from information security and privacy perspectives was proposed in 2010. A volunteer group has been formed to follow up on the project. The volunteer group consists of representatives from Australia, Canada, Germany, Japan, the Republic of Korea, the Netherlands, Sweden, Turkey, The United Kingdom, The United States of America and The European Union, and the Committees to the OECD (including the Business and Industry Advisory Committee, Civil Society Information Society Advisory Committee and the Internet Technical Advisory Committee). The Republic of Korea will be participating in this project and will also be providing financial support.

WPISP work on privacy: The "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" issued in 1980 represent an international consensus on the handling of personal information in the public and private sectors. "Privacy Online: OECD Guidance on Policy and Practice" issued in 2002 focuses on privacy-enhancing technologies, online privacy policies, enforcement and redress, and the like in relation to e-commerce. At present, the WPISP is working on Privacy Law Enforcement Cooperation.

The project to develop indicators on information security and privacy for reliable and comparative statistics among OECD members was proposed in 2011. The Republic of Korea will contribute to this project through active participation and financial support.

Other work: In 1998, the OECD issued the "Guidelines on Cryptography Policy" and held the Ottawa Ministerial Declaration on Authentication for Electronic Commerce. A "Survey of Legal and Policy Frameworks for E-Authentication Services and e-Signatures in OECD Member Countries" was conducted from 2002 to 2003. In 2005, "The Use of Authentication across Borders in OECD Countries" was announced.

In 2004, "Biometric-Based Technologies" was written, and in 2005, the taskforce on spam was formed. Other ongoing work relates to digital identity management, malware, pervasive radio frequency identification (RFID), sensors and networks, and a common framework for implementing information security and privacy.

[40] OECD, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002). Paris, France. https://www.oecd.org/digital/ieconomy/15582260.pdf.

[41] Ibid., p. 8.

Information security activities of APEC[42]

The Asia-Pacific Economic Cooperation (APEC) is pursuing information security activities in the Asia-Pacific region through the Telecommunications and Information Working Group (TEL), which consists of three steering groups: the Liberalization Steering Group, ICT Development Steering Group, and Security and Prosperity Steering Group.

Especially since the Sixth APEC Ministerial Meeting on the Telecommunications and Information Industry held in Lima, Peru in June 2005, the Security and Prosperity Steering Group has stepped up discussions on cybersecurity and cybercrime. The APEC Cyber-Security Strategy, which includes strengthening consumer trust in the use of e-commerce, serves to unify the efforts of various economies. These efforts include enacting and implementing laws on cybersecurity that are consistent with the United Nations General Assembly Resolution 55/63[43] and the Convention on Cybercrime.[44] The TEL Cybercrime Legislation Initiative and Enforcement Capacity Building Project will support institutions in implementing new laws.

APEC members are also working together to implement CERTs as an early warning defense system against cyberattacks. The Republic of Korea is providing training to developing country members, and guidelines for establishing and operating CERTs have been developed.

The protection of SMEs and home users from cyberattacks and viruses is considered a priority and a number of tools have been developed for this purpose. Information is being provided on how to use the Internet securely, and on safety issues relating to wireless technologies and safe e-mail exchanges.

Reducing the criminal misuse of information through information sharing, development of procedures and mutual assistance laws, and other measures to protect business and citizens, will continue to be a priority for the APECTEL. As part of its agenda on security issues, the APECTEL approved in 2007 the “Guide on Policy and Technical Approach against Botnet” and the Workshop on Cyber Security and Critical Information Infrastructure.

As endorsed by the APEC Counter-Terrorism Task Force (CTTF) and APECTEL in 2009, the “Third APEC Seminar on the Protection of Cyberspace to Better Defend Our Economies through IT Security” was held in Seoul, Republic of Korea on 7-8 September 2011 with 86 of delegates, moderator and speakers from 16 economies. The Seminar was hosted by the Ministry of Foreign Affairs and Trade, Ministry of Public Administration and Security, and the KCC, and sponsored by the Korea Internet & Security Agency (KISA).

---

[42] *Telecommunications and Information*. Asia-Pacific Economic Cooperation. (2020, April). https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.

[43] “Combating the criminal misuse of information”, which recognizes that one of the implications of technological advances is increased criminal activity in the virtual world.

[44] An Agreement undertaken in Budapest that aims to uphold the integrity of computer systems by considering as criminal acts any action that violates said integrity. See http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

The Seminar was a follow-up activity to the two previous CTTF-TEL joint projects, namely the "APEC Training Program for a Strengthened Cyber Security in the Asia-Pacific Region" held on 15-30 November 2007, in Seoul, and the "APEC Seminar on Protection of Cyberspace from Terrorist Use and Attacks" held on 26-27 June 2008, in Seoul. Building on the outcomes of the training programme and the first seminar, the third seminar brought together government officials and experts from APEC member economies to address various cybersecurity issues including protection of critical infrastructure from terrorist attacks.

Information security activities of the ITU[45]

The ITU is the leading United Nations agency for ICTs. Based in Geneva, Switzerland, the ITU has 191 member States and more than 700 sector members and associates.

The ITU's role in helping the world communicate spans three core sectors. The Radiocommunication Sector (ITU-R) focuses on managing the international radio frequency spectrum and satellite orbit resources. The Telecommunication Standardization Sector (ITU-T) focuses on standardization of information-communication networks and services. The Development Sector (ITU-D) was established to help spread equitable, sustainable and affordable access to ICT as a means of stimulating broader social and economic development. The ITU also organizes telecommunications-related events and was the lead organizing agency of the WSIS.

A fundamental role of ITU following WSIS is to build confidence and security in the use of ICTs. At WSIS, Heads of States and world leaders entrusted the ITU to take the lead in coordinating international efforts in the field of cybersecurity, as the sole facilitator of Action Line C.5, "Building confidence and security in the use of ICTs". Cybersecurity is one of the key focus areas under ITU-D.

The focus areas of WSIS Action Line C.5 are:

- CIIP
- Promotion of a global culture of cybersecurity
- Harmonizing national legal approaches, international legal coordination and enforcement
- Countering spam
- Developing watch, warning and incident response capabilities
- Information sharing of national approaches, good practices and guidelines
- Privacy, data and consumer protection

The ITU Global Cybersecurity Agenda (GCA) is an ITU framework for international cooperation aimed at proposing solutions to enhance confidence and security in the information society. GCA has five strategic pillars, also known as work areas:

- Legal Measures
- Technical & Procedural Measures

[45] International Telecommunications Union. (2021). ITU Cybersecurity Activities. http://www.itu.int/en/action/cybersecurity/Pages/default.aspx.

- Organizational Structures
- Capacity Building
- International Cooperation

The strategies are elaborated through the following goals:

- Develop a model cybercrime legislation that is globally applicable and interoperable with existing national/regional legislative measures
- Create national and regional organizational structures and policies on cybercrime
- Establish globally accepted minimum security criteria and accreditation schemes for software applications and systems
- Create a global framework for watch, warning and incident response to ensure cross-border coordination of initiatives
- Create and endorse a generic and universal digital identity system and the necessary organizational structures to ensure the recognition of digital credentials for individuals across geographical boundaries
- Develop a global strategy to facilitate human and institutional capacity building to enhance knowledge and know-how across sectors and in all of the above-mentioned areas
- Advise on a potential framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all of the above-mentioned areas

The GCA has fostered initiatives such as the Child Online Protection Initiative through its partnership with IMPACT and with the support of leading global players.

Another initiative is the ITU Cybersecurity Gateway that aims to provide an easy-to-use and interactive information resource on initiatives that are related to national and international cybersecurity. It is available to citizens, governments, businesses and international organizations. Services provided by the Gateway include information sharing, watch and warning, laws and legislation, privacy and protection, and industry standards and solutions.

The ITU-D also oversees the ITU Cybersecurity Work Programme that was established to help countries develop technologies for high-level security of cyberspace. It provides assistance related to the following:

- Establishing national strategies and capabilities for cybersecurity and CIIP
- Establishing appropriate cybercrime legislation and enforcement mechanisms
- Establishing watch, warning and incident response capabilities
- Countering spam and related threats
- Bridging the security-related standardization gap between developing and developed countries
- Establishing an ITU Cybersecurity/CIIP Directory, contact database and Who's Who publication
- Setting cybersecurity indicators
- Fostering regional cooperation activities
- Information sharing and supporting the ITU Cybersecurity Gateway
- Outreach and promotion of related activities

Other ITU-D cybersecurity-related activities are joint activities with StopSpamAlliance.org; regional capacity building activities on cybercrime legislation and enforcement; and development and distribution of resources and toolkits, including a botnet mitigation toolkit,[46] a toolkit for model cybercrime legislation for developing countries, a national cybersecurity self-assessment toolkit,[47] and cybersecurity/cybercrime publications and papers.[48]

The ITU-T sector is also contributing to the area of cybersecurity through its development of over 70 security-related standards (ITU-T Recommendations). Recently at a cybersecurity symposium, participants asked ITU-T to accelerate its work in this area, and in response, ITU-T is now giving added emphasis to the development of security standards. To assist in this process, ITU-T developed an "ICT Security Standards Road Map" that brings together information about existing standards, standards under development and future areas of security standards work.[49]

Standardization work is carried out by the technical study groups (SGs) in which representatives of the ITU-T membership develop recommendations (standards) for the various fields of international telecommunications. The SGs drive their work primarily in the form of study questions. Each question addresses technical studies in a particular area of telecommunication standardization.

Within ITU-T, Study Group 17 (SG17)[50] coordinates security-related work across all study groups.

SG17 is responsible for studies relating to security including cybersecurity, countering spam and identity management. It is also responsible for the application of open system communications including directory and object identifiers, and for technical languages, the method for their usage and other issues related to the software aspects of telecommunication systems.

The SG17 structure for study period 2017-2020 is as follows:

- Working Party 1. Telecommunication/ICT Security
    - Question 1 - Telecommunication/ICT security coordination

[46] Ramasubramanian, S., & Shaw, R. (2007, September). ITU Botnet Mitigation Project: Background & Approach. International Telecommunication Union. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit.pdf

[47] ITU-D ICT Applications and Cybersecurity Division. (2009). ITU National Cybersecurity/CIIP Self-Assessment Tool. http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

[48] International Telecommunications Union. (2021). *ITU-D Cybersecurity*. ITU-D. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx.

[49] International Telecommunication Union. ICT Security Standards Roadmap. http://www.itu.int/ITU-T/studygroups/com17/ict/index.html.

[50] International Telecommunications Union. *SG17 - Study Group Structure (Study Period 2017-2020)*. ITU. http://www.itu.int/net4/ITU-T/lists/sgstructure.aspx?Group=17&Period=16.

    - Question 2 – Security architecture and framework
    - Question 3 – Telecommunication information security management
    - Question 4 – Cybersecurity
    - Question 5 – Countering spam by technical means
- Working Party 2. Cyberspace security
    - Question 6 – Security aspects of ubiquitous telecommunication services
    - Question 7 – Security application services
    - Question 8 – Service oriented architecture security
    - Question 9 - Telebiometrics
- Working Party 3. Application security
    - Question 10 - Identity management architecture and mechanisms
    - Question 11 - Directory services, directory systems, and public key/attribute certificates
    - Question 12 - Abstract Syntax Notation One (ANS.1), Object Identifiers and associated registration
    - Question 13 - Formal languages and telecommunication software
    - Question 14 - Testing languages, methodologies and framework
    - Question 15 - Open Systems Interconnection

Work to build confidence and security in the use of information and communication technologies (ICTs) continues to intensify in a bid to facilitate more secure network infrastructure, services and applications. Over 170 standards (ITU-T Recommendations and Supplements) focusing on security have been published.

ITU-T Study Group 17 (SG17) coordinates security-related work across all ITU-T Study Groups. Often working in cooperation with other standards development organizations (SDOs) and various ICT industry consortia, SG17 deals with a broad range of standardization issues.

To give a few examples, SG17 is currently working on cybersecurity; security management; security architectures and frameworks; countering spam; identity management; the protection of personally identifiable information; and the security of applications and services for the Internet of Things (IoT), smart grid, smartphones, software defined networking (SDN), web services, big data analytics, social networks, cloud computing, mobile financial systems, IPTV and telebiometrics.

One key reference for security standards in use today is the ITU-T Recommendation X.509 for electronic authentication over public networks. X.509 is used for designing applications related to public key infrastructure, and is widely used in a wide range of applications from securing the connection between a browser and a server on the Web to providing digital signatures that enable e-commerce transactions. Another achievement of SG17 is Recommendation X.805, which will give telecommunications network operators and enterprises the ability to provide an end-to-end architecture description from a security perspective.[51]

SG 17 is also the place to study technical languages and description techniques. An example is the formal language ASN.1, an important component for protocol specification or systems

[51] International Telecommunications Union. Study Group 17 at a glance. http://www.itu.int/net/ITU-T/info/sg17.aspx.

design. ASN.1 is an extremely important part of today's networks. ASN.1 is used, for example, in the signaling system for most telephone calls, package tracking, credit card verification and digital certificates and in many of the most used software programs. And today's work is progressing towards the development of unified modeling language profiles for ITU-T languages.[52]

Information security activities of the ISO/IEC

An Information Security Management System (ISMS) is, as the name suggests, a system for managing information security. It consists of processes and systems to ensure confidentiality, integrity and availability of information assets while minimizing security risks. 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 states the requirements for establishing an ISMS, and IS 17799: 2000, published as IS 17799:2005, stipulates basic controls for implementing an ISMS.

The de facto ISMS standard was the BS 7799, which was first developed by the British Standards Institution (BSI) in 1995 as the code of practice for information security management. In 1998, as the requirements specification was developed based on this standard, "the code of practice for information security management" was changed to Part 1 and the requirements specification became Part 2. Part 1 specifies controls for information security management, while Part 2 states the requirements for establishing an ISMS and describes the information security process (Plan-Do-Check-Act Cycle) for the continuous improvement of the base of risk management.

Part 1 was established as IS 17799 by the ISO/IEC JTC 1/SC27 WG1 in 2000. Since then, IS 17799 has been reviewed (with over 2,000 comments) and revised, and the final version was registered to the international standard in November 2005. IS 17799: 2000 provides 126 controls within 10 domains. IS 17799 revised in 2005 provides 11 administrative control domains and 133 controls.

Part 2 of BS 7799 established in 1999 had been used as the standard for ISMS certification. It was revised in September 2002 to align with ISO 9001 and ISO 14001, among others. The ISO adopted BS7799 Part 2: 2002 through the fast track method for coping with requests for the international standardized ISMS and registered it as the international standard ISO27001 by revising it slightly within a short time. The prominent changes made include adding content about effectiveness and modifying the appendix.

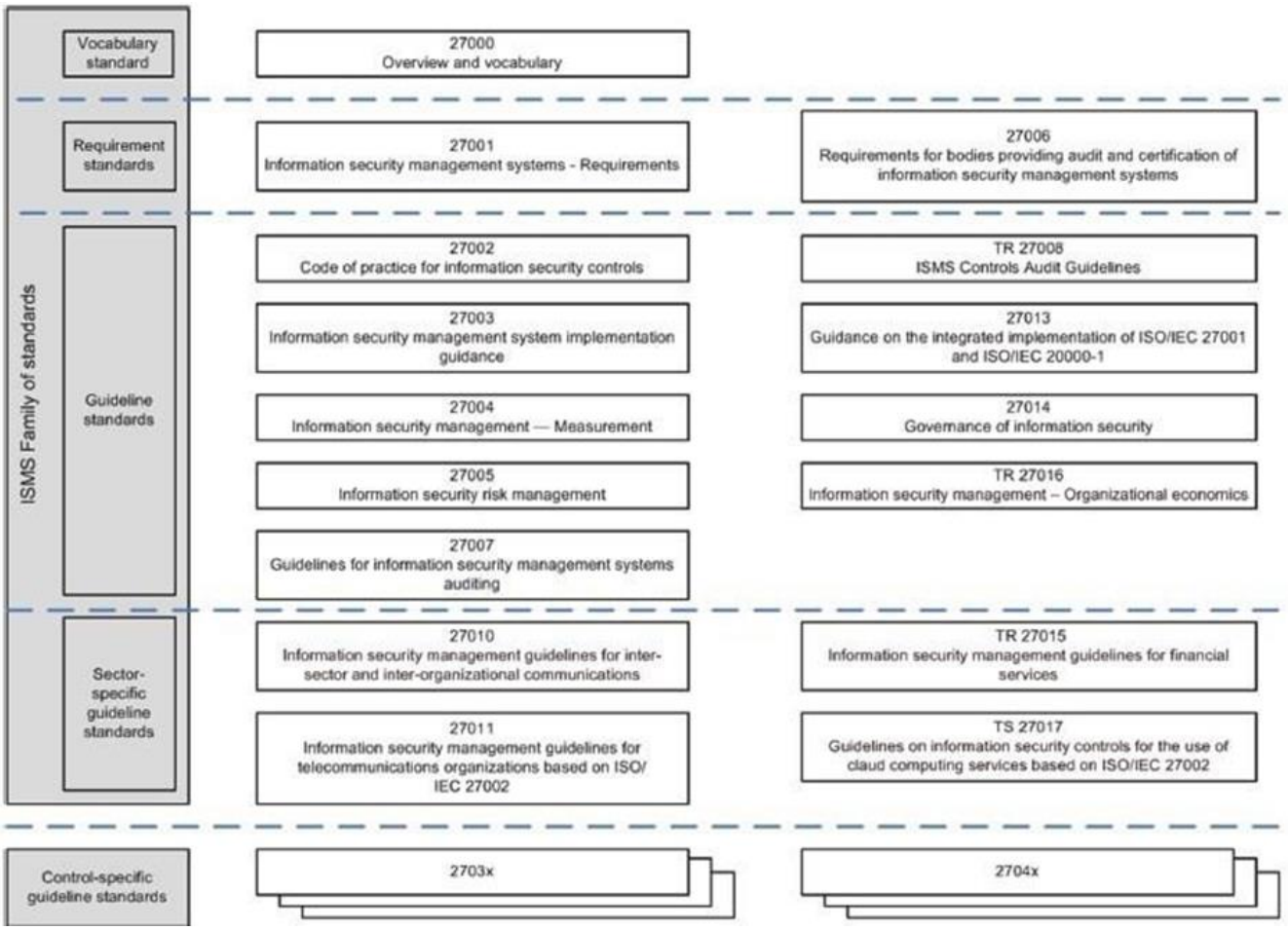
As the two important documents related to ISMS have been standardized internationally, a family of international security standards has emerged under the 27000 serial number scheme,

[52] Ibid.

which is the same as the other management systems (Quality business: 9000 series, Environmental management: 14000 series). IS 27001, the revised version of IS 17799:2005, embodies the requirements for establishing an ISMS and IS17799:2005, which includes the basic controls for implementing ISMS, has been changed to IS27002 in 2007. Guidance for the implementation of an ISMS, a standard for information security risk management, and information security management measurement developed by JTC1 SC27 are in the 27000 series.

Figure 9 shows the family of ISMS-related standards. ISMS certification activities are gaining momentum and it is expected that ISMS standards or guidelines that are appropriate to specific industries are being developed based on the common ISMS for general systems. An example is the effort to develop ISMS guidelines reflecting the characteristics of the communications industry.

Figure 9: ISO/IEC 27000 family



Questions to Think About

Which of the information security activities being spearheaded by international organizations have been or are being adopted in your country? How are they being implemented?

Test Yourself

1. What are the similarities among the information security activities being undertaken by the countries included in this section? What are their differences?

2. What are the information security priorities of the international organizations included in this section?

4. Information Security Methodology

This section aims to describe internationally used administrative, physical and technical information security methodology.

4.1. Different Aspects of Information Security

Information security methodology aims to minimize damage and maintain business continuity considering all possible vulnerabilities and threats to information assets. To guarantee business continuity, information security methodology seeks to ensure the confidentiality, integrity and availability of internal information assets. This involves the application of risk assessment methods and controls. Essentially, what is needed is a good plan that covers the administrative, physical and technical aspects of information security.

Administrative aspect

There are many ISMSs that focus on the administrative aspect. ISO/IEC27001 is one of the most commonly used ISMS standards.

ISO/IEC27001, the international ISMS standard, is based on BS7799, which was established by BSI. BS7799 specifies requirements to implement and manage an ISMS and common standards applied to security standards of various organizations and effective security management. Part 1 of BS7799 describes the required security activities based on the best practices of security activities in organizations. Part 2, which has become the present ISO/IEC27001, suggests the minimum requisites needed for ISMS operation and assessment of security activities.

The security activities in ISO/IEC27001 consist of 114 controls in 14 clauses (see table 5).

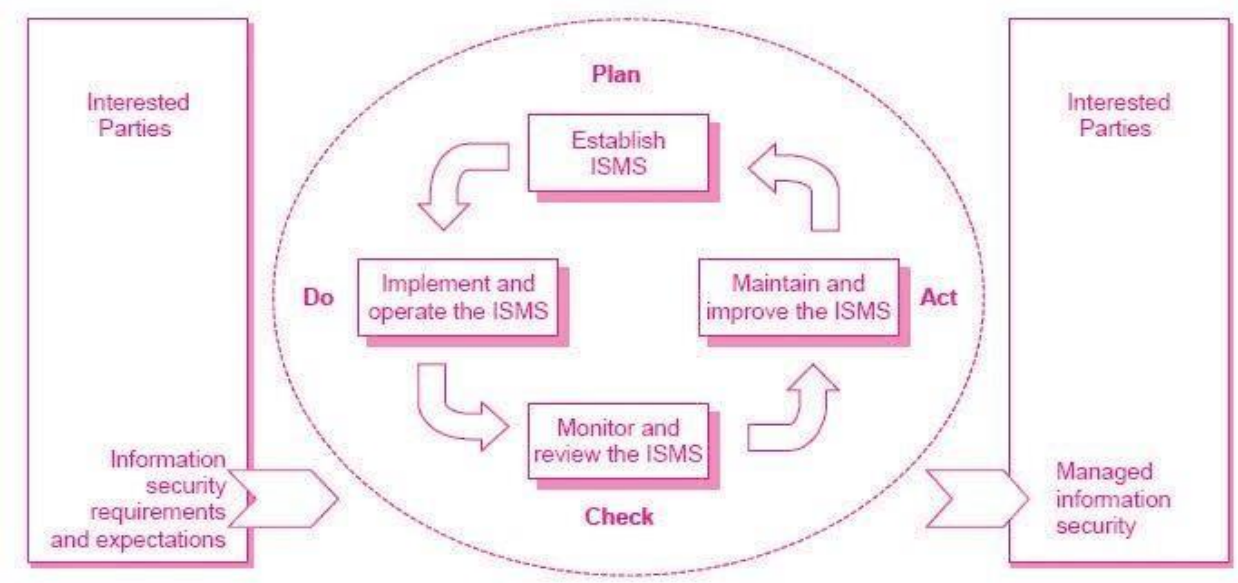
Table 5: Controls in ISO/IEC27001

Domains	Items
A5.	Information Security policies
A6.	Organization of information security
A7.	Human resource security
A8.	Asset management
A9.	Access control
A10.	Cryptography
A11.	Physical and environmental security
A12.	Operations security

A13.	Communications security
A14.	System acquisition, development and maintenance
A15.	Supplier relationships
A16.	Information security incident management
A17.	Information security aspects of business continuity management
A18.	Compliance

ISO/IEC27001 adopts the Plan-Do-Check-Act process model, which is applied to structure all ISMS processes. In ISO/IEC27001, all evidence of the ISMS assessment should be documented; the certification should be externally audited every six months; and the whole process should be repeated after three years in order to continuously manage the ISMS.

Figure 10: Plan-Do-Check-Act process model applied to ISMS processes



Source: ISO/IEC JTC 1/SC 27.

Security controls should be planned considering the security requirements. All human resources, including suppliers, contractors, customers and outside specialists, should participate in these activities. Setting up security requirements is based on the following three factors:

- Risk assessment
- Legal requirements and contract clauses
- Information processes for operating the organization

Gap analysis refers to the process of measuring the current information security level and establishing the future direction of information security. The result of the gap analysis is derived from the asset owners' answers to the 133 controls and 11 domains. Once deficient areas are identified through the gap analysis, the appropriate controls per area can be established.

Risk assessment is divided into the assessment of asset value and assessment of threats and vulnerabilities. Asset value assessment is a quantitative valuation of information assets. The threat assessment involves rating threats to the confidentiality, integrity and availability of information. The example below shows the computations involved in risk assessment.

Asset name	Asset value	Threat			Vulnerability			Risk		
		C	I	A	C	I	A	C	I	A
Asset name #1	2	3	3	1	3	1	1	8	6	5

- Asset Value + Threat + Vulnerability = Risk
- Confidentiality: Asset Value(2) + Threat(3) + Vulnerability(3) = Risk(8)
- Integrity: Asset Value(2) + Threat(3) + Vulnerability(1) = Risk(6)
- Availability: Asset Value(2) + Threat(1) + Vulnerability(1) = Risk(5)

Application of controls: Each risk value will be different according to the result of the risk assessment. Decisions are needed to apply the appropriate controls to the differently valued assets. Risks should be divided into acceptable risks and unacceptable risks according to the Degree of Assurance criterion. Controls will need to be applied to information assets with unacceptable risk. The controls are applied based on the ISO/IEC controls, but it is more effective to apply controls depending on the real state of the organization.

Technical aspect

There is no ISMS for technical aspects. International common evaluation standards such as the Common Criteria (CC) certification[53] may be used instead.

CC certification has commercial roots. It was established to address concerns about differences in security levels of IT products from different countries. The international standard was established for the evaluation of IT products by Canada, France, Germany, the United Kingdom and the United States of America.

Specifically, the CC presents requirements for the IT security of a product or system under the distinct categories of functional requirements and assurance requirements. CC functional requirements define desired security behaviour. Assurance requirements are the basis for gaining confidence that the claimed security measures are effective and implemented correctly. CC security functions consist of 134 components from 11 classes made up of 65 families. The assurance requirements refer to 81 components from eight classes made up of 38 families.

Security functional requirement (SFR): The SFRs specify all security functions for the Target of Evaluation (TOE). Table 6 lists the classes of security functions included in SFRs.

[53] Common Criteria. Common Criteria : New CC Portal. http://www.commoncriteriaportal.org/.

Table 6: Composition of class in SFRs

Classes		Details
FAU	Security audit	Refers to functions that include audit data protection, record format and event selection, as well as analysis tools, violation alarms and real-time analysis
FCO	Communication	Describes requirements specifically of interest for TOEs that are used for the transport of information
FCS	Cryptographic support	Specifies the use of cryptographic key management and cryptographic operation
FDP	User data protection	Specifies requirements related to protecting user data
FIA	Identification and authentication	Addresses the requirements for functions to establish and verify a claimed user identity
FMT	Security management	Specifies the management of several aspects of the TOE Security Functions (TSF): security attributes, TSF data and functions
FPR	Privacy	Describes the requirements that could be levied to satisfy the users' privacy needs, while still allowing the system flexibility as far as possible to maintain sufficient control over the operation of the system
FPT	Protection of the TSF	Contains families of functional requirements that relate to the integrity and management of the mechanisms that constitute the TSF and the integrity of TSF data
FRU	Resource utilization	Contains the availability of required resources such as processing capability and/or storage capacity
FTA	TOE access	Specifies functional requirements for controlling the establishment of a user's session
FTP	Trusted path/ channels	Provides requirements for a trusted communication path between users and the TSF

Source:
Common Criteria. (2009). (publication). *Common Criteria for Information Technology Security Evaluation*. Retrieved from https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf

Security assurance components (SACs): The CC philosophy requires the articulation of security threats and commitments to organizational security policy through appropriate and adequate security measures. The measures to be adopted should help identify vulnerabilities, reduce the likelihood of being exploited and reduce the extent of damage in the event that a vulnerability is exploited.[54] Table 7 lists the classes included in SACs.

Table 7: Composition of class in SACs

Classes		Details
APE	Protection Profile (PP) evaluation	This is required to demonstrate that the PP is sound and internally consistent and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages.
ASE	Security Target (ST) evaluation	This is required to demonstrate that the ST is sound and internally consistent and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages.
ADV	Development	This provides information about the TOE. The knowledge obtained is used as the basis for conducting vulnerability analysis and testing upon the TOE, as described in the ATE and AVA classes.
AGD	Guidance documents	For the secure preparation and operation of the TOE, it is necessary to describe all relevant aspects for the secure handling of the TOE. The class also addresses the possibility of unintended incorrect configuration or handling of the TOE.
ALC	Life cycle support	In the product life cycle, which includes configuration management (CM) capabilities, CM scope, delivery, development security, flaw remediation, life cycle definition, tools and techniques, it is distinguished whether the TOE is under the responsibility of the developer or the user.
ATE	Tests	The emphasis in this class is on confirmation that the TSF operates according to its design descriptions. This class does not address penetration testing.

[54] Common Criteria. (2009). (publication). *Common Criteria for Information Technology Security Evaluation*. Retrieved from https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf

.

AVA	Vulnerability assessment	The vulnerability assessment activity covers various vulnerabilities in the development and operation of the TOE.
ACO	Composition	Specifies assurance requirements that are designed to provide confidence that a composed TOE will operate securely when relying upon security functionality provided by previously evaluated software, firmware or hardware components.

Source:
Common Criteria. (2009). (publication). *Common Criteria for Information Technology Security Evaluation*. Retrieved from https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf

Evaluation method of CC

1. **Evaluation of PP (APE)**: The PP describes implementation-independent sets of security requirements for categories of TOE and contains a statement of the security problem that a compliant product is intended to solve. It specifies CC functional and assurance requirements and provides a rationale for the selected functional and assurance components. It is typically created by a consumer or consumer community for IT security requirements.

2. **Evaluation of ST (ASE)**: The ST is the basis for the agreement between the TOE developers, consumers, evaluators and evaluation authorities as to what security the TOE offers, and the scope of the evaluation. The audience for an ST may also include those managing, marketing, purchasing, installing, configuring, operating and using the TOE. An ST contains some implementation-specific information that demonstrates how the product addresses the security requirements. It may refer to one or more PPs. In this case, the ST must fulfil the generic security requirements given in each of these PPs and may define further requirements.

3. **Others**: Evaluation of ADV, AGD, ALC, ATE, AVA and ACO.

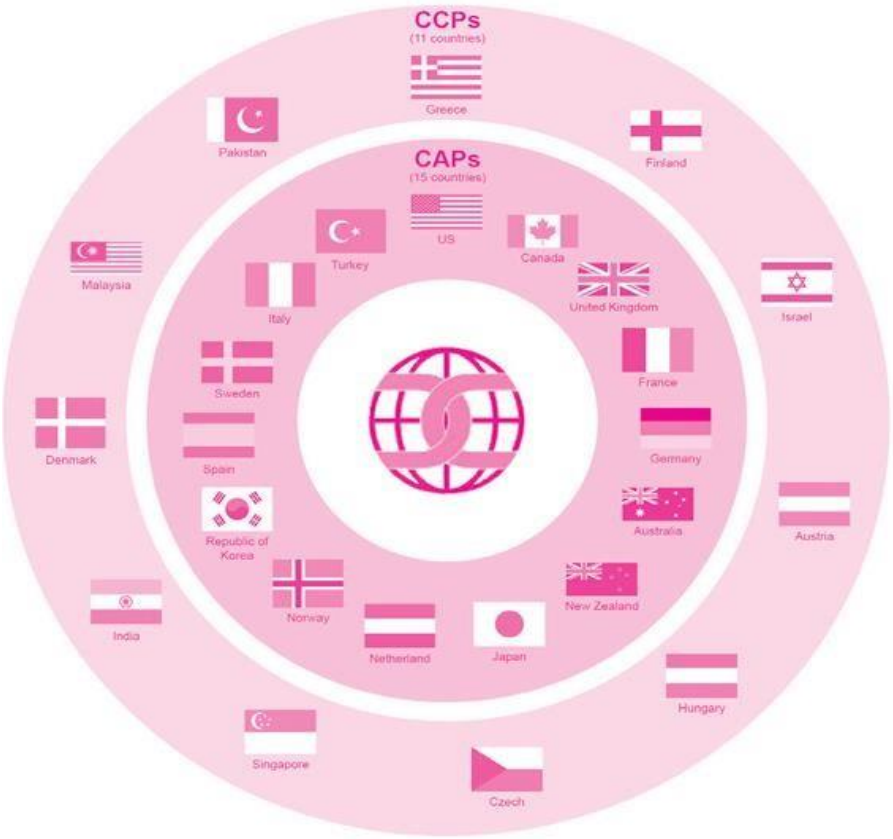
Common Criteria Recognition Arrangement

The Common Criteria Recognition Arrangement (CCRA) was organized for approving CC certifications among nations. It aims to ensure that CC evaluations are performed to consistent standards, eliminate or reduce duplicate evaluations of IT products or protection profiles, and improve global market opportunities for the IT industry by approving certification among member nations.

The CCRA consists of 26 member nations, of which 15 are Certificate Authorizing Participants (CAPs) and 11 are Certificate Consuming Participants (CCPs). CAPs are producers of evaluation certificates. They are the sponsors of a compliant certification body operating in their own country and they authorize the certificates issued. A country must be a member of the CCRA as CCP for a minimum period of two years before it can apply to become a CAP. CCPs

are the consumers of evaluation certificates. Although they may not maintain an IT security evaluation capability, they have an expressed interest in the use of certified/validated products and protection profiles. To become a member of the CCRA, a country should submit a written application to the Management Committee.

Figure 11: CAPs and CCPs



4.2. Examples of Information Security Methodology

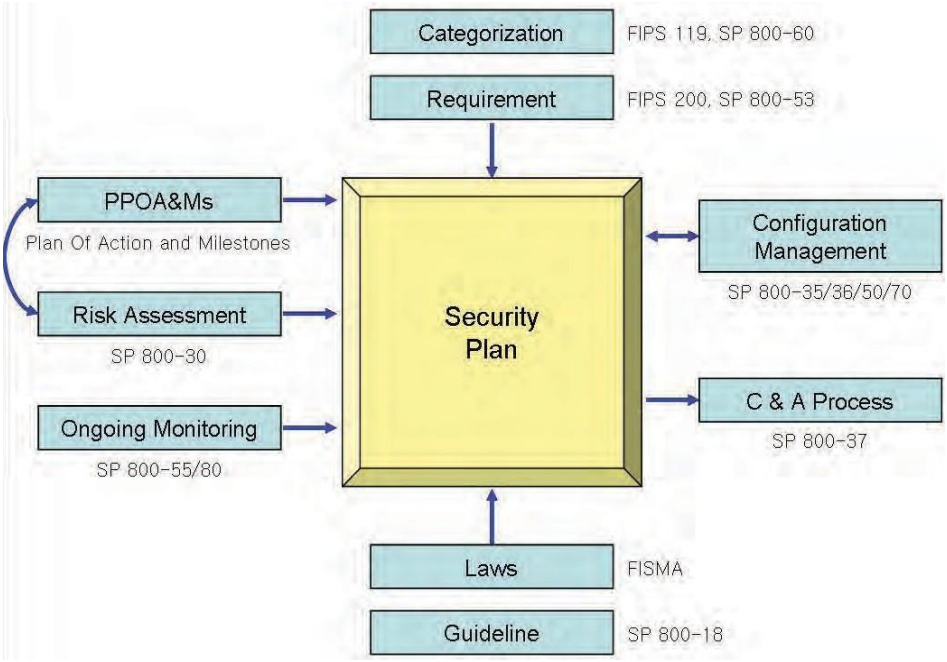
The United States of America's National Institute of Standards and Technology

Based on FISMA, the United States of America's National Institute of Standards and Technology (NIST) has developed guidelines and standards for strengthening the security of information and information systems that Federal institutes are able to use. The guidelines and standards aim to:

- Provide a specification for minimum security requirements by developing standards that can be used for categorization of Federal information and information systems;
- Enable security categorization of information and information systems;
- Select and specify security controls for information systems supporting the executive agencies of the Federal government; and
- Verify the efficiency and effectiveness of security controls on vulnerabilities.

Guidelines related to FISMA are published as special publications and Federal Information Processing Standards Publications. There are two series of special publications: the 500 series for information technology and the 800 series for computer security. Figure 12 shows the process that the United States of America's government agencies follow to establish their security plans based on this standard.

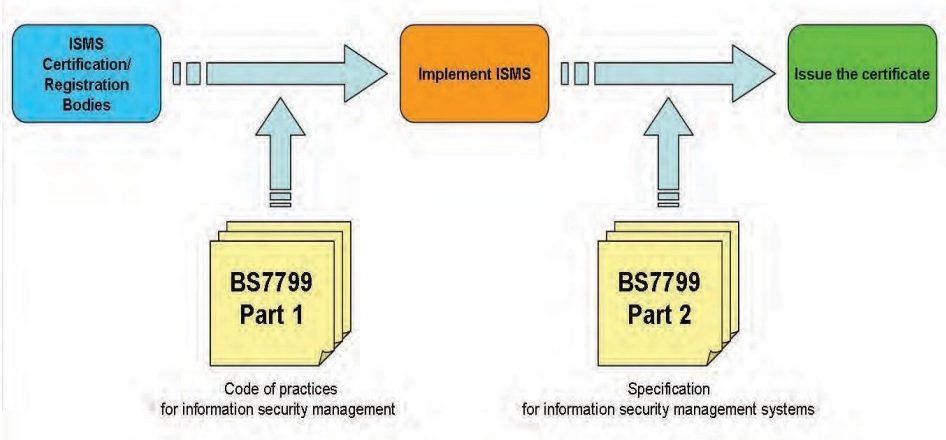
Figure 12: Security planning process input/output



United Kingdom (BS7799)

As mentioned earlier, BSI analyses the security activities of organizations in the United Kingdom and gives BS7799 certification, which has now been developed to ISO27001 (BS7799 part 2) and ISO27002 (BS7799 part 1). Figure 13 shows the procedure that is followed.

Figure 13: BS7799 certification process



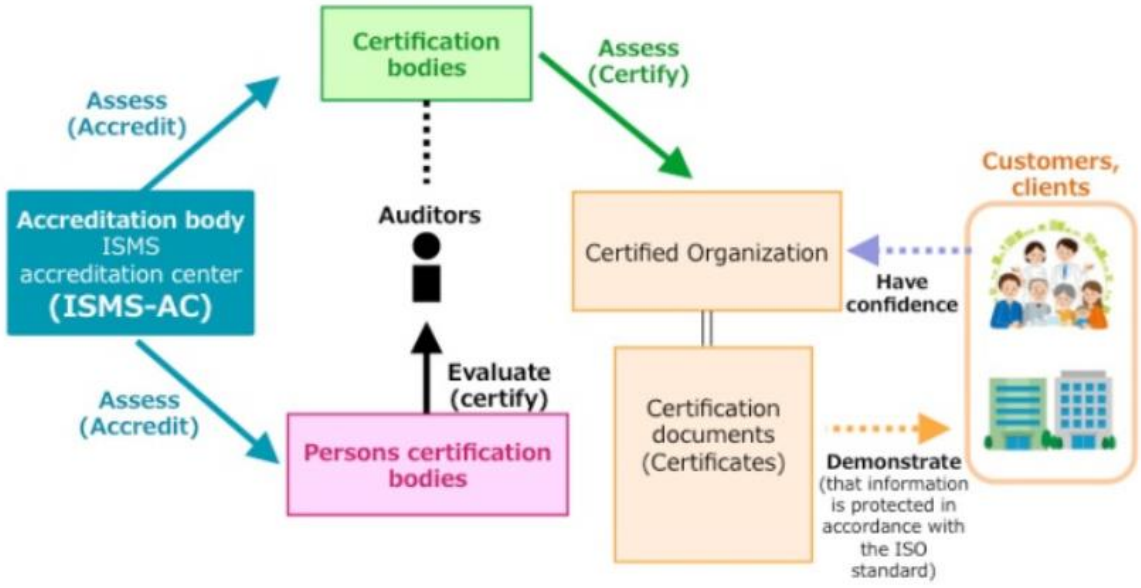
Japan (from ISMS Ver2.0 to JIS Q 27001:2014)[55]

ISMS Ver2.0 of the Japan Information Processing Development Corporation has operated in Japan since April 2002. Since then, it has been replaced by BS7799 Part 2: 2002, JIS Q 27001:2006 in March 2006 in line with the publication of ISO/IEC 27001:2005, and then revised and issued in March 2014 as JIS Q 27001:2014 according to the revision of ISO/IEC 27001.

The ISMS conformity assessment scheme in Japan has a comprehensive structure composed of "certification bodies" that assess and certify an applicant organization's ISMS based on ISO/IEC 27001, "personnel certification bodies" that certify and register ISMS auditors, and the "accreditation body" that assesses the competence of those bodies in implementing such tasks. With regard to "auditor training bodies", the personnel certification bodies carry out the assessment of those bodies and approve them based on the result of the assessment.

Figure 14 shows the ISMS certification system in Japan.

Figure 14: ISMS certification system in Japan



Source : ISMS Accreditation Centre. Overview of the ISMS conformity assessment scheme. ISMS-AC. https://isms.jp/english/isms/about.html.

Republic of Korea (KISA ISMS)

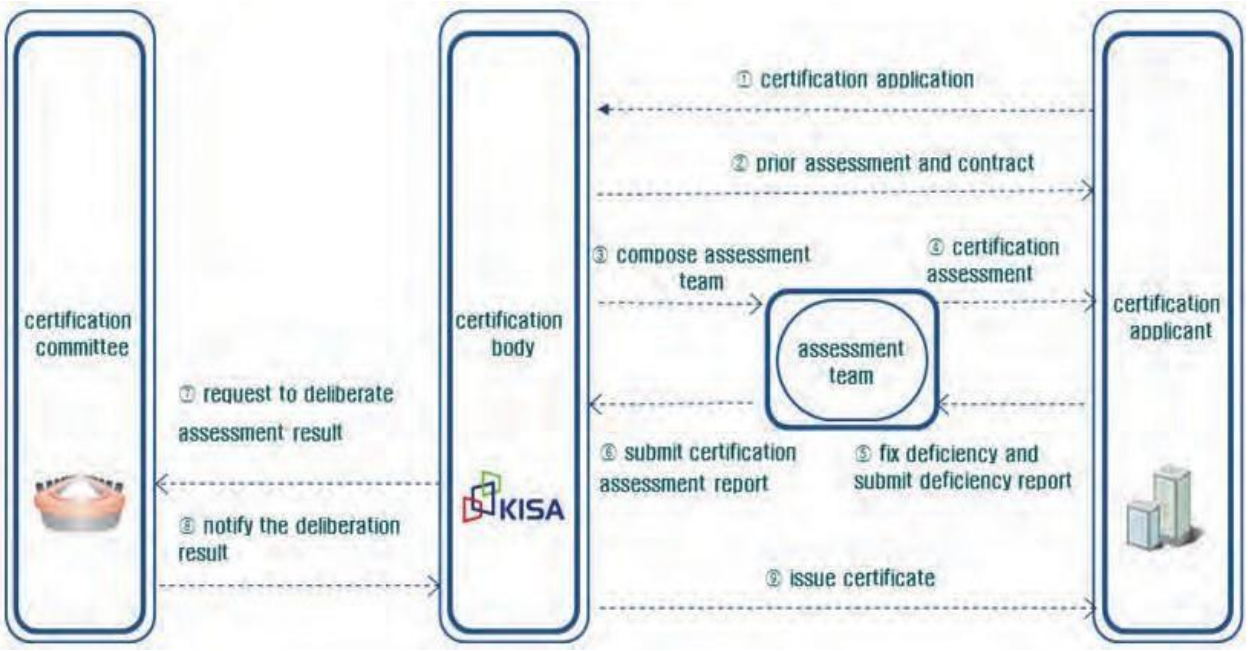
Since 2002, KCC and KISA have introduced and operated an ISMS certification programme. KCC and KISA have made great effort to promote the ISMS certification programme, and today it is considered a very successful programme. The ISMS certification scheme and procedures

[55] ISMS Accreditation Centre. *Overview of the ISMS conformity assessment scheme*. ISMS-AC. https://isms.jp/english/isms/about.html.

are shown in figures 15 and 16 respectively. In 2011, the number of ISMS certificates reached 114. As the number has increased, the information security level of each certified organizations has been expected to increase dramatically. The certified organizations include the leading companies in various business fields such as KT, Korean Air, NHN, Daum, among others.

Figure 15: ISMS certification scheme in the Republic of Korea

Figure 16: ISMS certification procedures in the Republic of Korea



Germany

Germany's BSI (Bundesamt fűr Sicherheit in der Informationstechnik) is the national agency for information security. The BSI is first and foremost the central IT security service provider for the

federal government in Germany. It provides IT security services to the German government, cities, organizations and individuals in Germany.

BSI has established the IT Baseline Protection Qualification based on the international standard, ISO Guide 25[GUI25] and the European standard, EN45001, which is acknowledged by the European Committee for IT Testing and Certification. The certification types include IT Baseline Protection Certificate, Self-declared (IT Baseline Protection higher level) and Self-declared (IT Baseline Protection entry level). In 1999, the EN45001 was replaced with the ISO / IEC / EN 17025.

In addition, the Baseline protection manual (BPM) and sub-manual BSI Standard Series:100-X have been developed. The matter includes BSI Standard 100-1 ISMS, BSI Standard 100-2 BPM Methodology and BSI Standard 100-3 Risk analysis.

In 2011, Germany officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI, BKA (Federal Police Organisation), BND (Federal Intelligence Service), MAD (Military Intelligence Service) and other national organisations in Germany taking care of national security aspects. The primary task of NCAZ is to detect and prevent attacks against the national infrastructure. Germany has also established the largest research institution for IT security in Europe, the Center for Research in Security and Privacy (CRISP) in Darmstadt.

Others

Table 8 lists other existing ISMS certifications.

Table 8: ISMS certification of other countries

	Accreditation Institutes	Standards
Canada	Communications Security Establishment	MG-4 A Guide to Certification & Accreditation for Information Technology Systems
Germany	DAkkS	
India	National Accreditation Board for Testing and Calibration Laboratories (NABL)	
Indonesia	Komite Akreditasi Nasional (KAN)	
Ireland	Irish National Accreditation Board (INAB)	

New Zealand	International Accreditation New Zealand (IANZ)	
Taiwan Province of China	Bureau of Standards, Meteorology and Inspection	CNS 17799 & CNS 17800
The Netherlands	Dutch Accreditation Council (DAC)	
Singapore	Information Technology Standards Committee	SS493: Part1 (IT Security Standard Framework) & SS493: Part 2 (Security Services) under development
Republic of Korea	Korea Laboratory Accreditation Scheme (KOLAS)	
Viet Nam	Bureau of Accreditation	

5. Protection of Privacy

This section aims to:
- Trace changes in the concept of privacy;
- Describe international trends in privacy protection; and
- Give an overview and examples of Privacy Impact Assessment

5.1. The Concept of Privacy

Personal information is any information relating to an identifiable individual[56] or an identified or identifiable natural person.[57] It includes information such as an individual's name, phone number, address, e-mail address, licence number of an automobile, physical characteristics (facial dimensions, fingerprints, handwriting, etc.), credit card number and family relationship.

Inappropriate access to and collection, analysis and use of an individual's personal information have an effect on the behaviour of others towards that individual, and ultimately have a negative impact on his/her social standing, property and safety. Therefore, personal information should be protected from improper access, collection, storage, analysis and use. In this sense, personal information is the subject of protection.

When the subject of protection is the right to personal information rather than the personal information itself, this is the concept of privacy. There are five ways to explain the right to privacy:

- The right to be free from unwanted access (e.g., physical access and access via short messaging service)
- The right not to allow personal information to be used in an unwanted way (e.g., sale of information, exposure of information and matching)
- The right not to allow personal information to be collected by others without one's knowledge and consent (e.g., through the use of CCTV and cookies)
- The right to have personal information expressed accurately and correctly (i.e. integrity)
- The right to get rewarded for the value of one's own information

The passive concept of privacy includes the right to be let alone and the natural right related to the dignity of human beings. It is connected to the law prohibiting trespass.

[56] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (1995). *Official Journal of the European Communities*, *38*(281), 31–50. https://doi.org/https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

[57] Organisation for Economic Co-operation and Development. *Privacy Online: OECD Guidance on Policy and Practice*. OECD. https://www.oecd.org/digital/ieconomy/privacyonlineoecdguidanceonpolicyandpractice.htm.

The active concept of privacy includes self-control of personal information or the right to manage/control personal information positively, including the right to make corrections to effects resulting from incorrect personal information.

5.2. Trends in Privacy Policy

OECD guidelines on protection of privacy

In 1980, the OECD adopted the "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," also known as the "OECD Fair Information Practices." In 2002 "Privacy Online: OECD Guidance on Policy and Practice" was announced.[58] The Guidelines apply to personal data, whether in the public or private sectors, that pose a danger to privacy and individual liberties because of the manner in which such information is processed, or because of its nature or the context in which it is used. The OECD principles identified in the Guidelines outline the rights and obligations of individuals in the context of automated processing of personal data, and the rights and obligations of those who engage in such processing. Furthermore, the basic principles outlined in the Guidelines are applicable at both the national and international levels.

The eight principles that make up the OECD guidelines on privacy protection are:

1. **Collection limitation principle**

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. **Data quality principle**

Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and up-to-date.

3. **Purpose specification principle**

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. **Use limitation principle**

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the purpose specification principle except with the consent of the data subject or by the authority of law.

[58] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 9–17 (2013). Paris, France. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

5. **Security safeguards principle**

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. **Openness principle**

There should be a general policy of openness about developments, practices and policies relating to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. **Individual participation principle**

An individual should have the right to:

a. Obtain from a data controller confirmation of whether the data controller has data relating to him/her;
b. Receive communication about data relating to him/her within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner, and in a form that is readily intelligible to him/her;
c. Be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
d. To challenge data relating to him/her and, if the challenge is successful, to have the data erased, rectified, completed or amended.

8. **Accountability principle**

A data controller should be accountable for complying with measures that give effect to the principles stated above.[59]

United Nations guidelines related to protection of privacy

Since the late 1960s, the world has paid attention to the effect on privacy of automated information processing. United Nations Educational, Scientific and Cultural Organization (UNESCO) in particular has shown interest in privacy and privacy protection since the "UN Guidelines for the Regulation of Computerized Personal Data File" was adopted by the General Assembly in 1990.

The United Nations Guidelines are applied to documents (papers) as well as computerized data files in the public or private sectors. The Guidelines establish a series of principles concerning

[59] UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files (1990). https://www.refworld.org/docid/3ddcafaac.html. Adopted by General Assembly resolution 45/95 of 14 December 1990. Contain procedures for implementing regulations concerning computerized personal data files.

minimum guarantees to be provided for national legislation or in the internal laws of international organizations, as follows:

1. **Principle of lawfulness and fairness**

Information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the United Nations.

2. **Principle of accuracy**

Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission, and that they are kept up to date regularly or when the information contained in a file is used, as long as they are being processed.

3. **Principle of purpose-specification**

The purpose that a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that:

a. All the personal data collected and recorded remain relevant and adequate to the purposes so specified;
b. None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified; and
c. The period for which the personal data are kept does not exceed that which would enable the achievement of the purposes so specified.

4. **Principle of interested-person access**

Everyone who offers proof of identity has the right to know whether information concerning him/her is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, to be informed of the addressees.

5. **Principle of non-discrimination**

Subject to cases of exceptions restrictively envisaged under principle 6, data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership in an association or trade union, should not be compiled.

6. **Power to make exceptions**

Departures from principles 1 to 4 may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, inter alia, the rights and

freedoms of others, especially persons being persecuted (humanitarian clause), provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system that expressly states their limits and sets forth appropriate safeguards.

Exceptions to principle 5 relating to the prohibition of discrimination, in addition to being subject to the same safeguards as those prescribed for exceptions to principles 1 and 4, may be authorized only within the limits prescribed by the International Bill of Human Rights and other relevant instruments in the field of the protection of human rights and the prevention of discrimination.

7. Principle of security

Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction, and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses.

8. Supervision and sanctions

The law of every country shall designate the authority that, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This authority shall offer guarantees of impartiality, independence vis-à-vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies.

9. Transborder data flows

When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands.

10. Field of application

The present principles should be made applicable, in the first instance, to all public and private computerized files and, by means of optional extension and subject to appropriate adjustments, to manual files. Special provisions, also optional, might be made to extend all or part of the principles to files on legal persons particularly when they contain some information on individuals.[60]

[60] Tan, D. R. (1999). Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United Stats and European Union. *Loyola of Los Angeles International and Comparative Law Review*, *21*(4). https://digitalcommons.lmu.edu/ilr/vol21/iss4/5.

Data privacy, ethics and protection was released by the United Nations Development Group (UNDG) and apply to UNDG entities.

This document sets out general guidance on data privacy, data protection and data ethics concerning the use of big data, collected in real time by private sector entities as part of their business offerings, and shared with UNDG members for the purposes of strengthening operational implementation of their programmes to support the achievement of the 2030 Agenda.

The guidance sets out as follows:

1. **Lawful, legitimate and fair use**

Data access, analysis or other use must be consistent with the United Nations Charter and in furtherance of the Sustainable Development Goals.

2. **Purpose specification, use limitation and purpose compatibility**

Any data use must be compatible or otherwise relevant, and not excessive in relation to the purposes for which it was obtained.

3. **Risk mitigation and risk, harms and benefits assessment**

A risk, harms and benefits assessment that accounts for data protection and data privacy as well as ethics of data use should be conducted before a new or substantially changed use of data is undertaken.

4. **Sensitive data and sensitive contexts**

Stricter standards of data protection should be employed while obtaining, accessing, collecting, analysing or otherwise using data on vulnerable populations and persons at risk, children and young people, or any other sensitive data.

5. **Data security**

Data security is crucial in ensuring data privacy and data protection. Taking into account available technology and cost of implementation, robust technical and organizational safeguards and procedures (including efficient monitoring of data access and data breach notification procedures) should be implemented to ensure proper data management throughout the data lifecycle and prevent any unauthorized use, disclosure or breach of personal data.

6. **Data retention and data minimization**

Data access, analysis or other use should be kept to the minimum amount necessary to fulfill its purpose. The amount of data, including its granularity, should be limited to the minimum necessary. Data use should be monitored to ensure that it does not exceed the legitimate needs of its use.

7. Data quality

All data-related activities should be designed, carried out, reported and documented with an adequate level of quality and transparency. More specifically, to the extent reasonably possible, data should be validated for accuracy, relevancy, sufficiency, integrity, completeness, usability, validity and coherence, and be kept up to date.

8. Open data, transparency and accountability

Appropriate governance and accountability mechanisms should be established to monitor compliance with relevant law, including privacy laws and the highest standards of confidentiality, moral and ethical conduct with regard to data use

9. Due diligence for third party collaborators

Third party collaborators engaging in data use should act in compliance with relevant laws, including privacy laws as well as the highest standards of confidentiality and moral and ethical conduct.

European Union Data Protection[61]

The European Union's Council of Ministers initially adopted the European Directive on the Protection of Individuals with Regard to Processing of Personal Data and on the Free Movement of Such Data (EU Directive 95/46/EC) on 24 October 1995 to provide a regulatory framework to guarantee secure and free movement of personal data across the national borders of European Union member countries, in addition to setting a baseline of security around personal information wherever it is stored, transmitted or processed.

This directive was repealed in April 2016 with Regulation (EU) 2016/679 which strengthens individuals' fundamental rights in the digital age and facilitates business by clarifying rules for companies and public bodies in the digital single market. A single law will also do away with the current fragmentation in different national systems and unnecessary administrative burdens. Regulation (EU) 2016/679 entered into force on 24 May 2016 and has applied since 25 May 2018.

Privacy protection in the United States of America

The US has entrusted privacy protection activities to the market since too many government restrictions have hampered e-commerce activities. As a result, privacy seals such as Trust-e or Better Business Bureau Online have emerged, and laws on protection of privacy are not integrated. The Privacy Act of 1974 provides for the protection of privacy of information in the

[61] EUR-Lex, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504.

public sector while different laws govern privacy in the private sector. There is no organization dealing with all privacy protection issues in the private sector. In the public sector, the Office of Management and Budget (OMB) plays a role in establishing the federal government's privacy policy according to the Privacy Act. In the private sector, the Federal Trade Commission is authorized to execute laws protecting children's online privacy, customer credit information and fair-trade practices.

The United States of America laws related to the protection of privacy include:

- The Privacy Act, 1974
- Consumer Credit Protection Act, 1984
- Electric Communications Privacy Act, 1986
- Health Insurance Portability and Accountability Act, 1996
- Children's Online Privacy Protection Act, 1998
- Gramm-Leach-Bliley Act, 1999
- Sarbanes-Oxley Act, 2002
- Federal Information Security Management Act, 2002

In addition, there are privacy regulations enacted for each of the states in the United States of America.

Questions to Think About

1. In your country, what policies and laws are in place to protect privacy of information?

2. What issues or considerations impact on the enactment and/or implementation of such policies and laws?

3. What principles (see the OECD Guidelines and the United Nations Guidelines) do you think underpin the policies and laws concerning privacy protection in your country?

5.3. Privacy Impact Assessment

What is PIA?

A Privacy Impact Assessment (PIA) is a systematic process of investigating, analysing and evaluating the effect on the customers' or the nation's privacy of the introduction of new information systems or the modification of existing information systems. PIA is based on the principle of preliminary prevention—i.e. prevention is better than cure. It is not simply a system evaluation but the consideration of the serious effects on privacy of introducing or changing new systems. Thus, it is different from the privacy protection audit that ensures the observance of internal policy and external requirements for privacy.

Because a PIA is conducted to analyse the privacy invasion factor when a new system is built, it should be performed at the early phase of development, when adjustments to development specifications are still possible. However, when a serious invasion risk occurs in collecting, using and managing personal information while operating the existing service, it would be desirable to perform a PIA and then modify the system accordingly.

The PIA process[62]

A PIA generally consists of three steps (see table 9).

[62] Information and Privacy Commissioner of Ontario, Planning for Success: Privacy Impact Assessment Guide (2015). https://www.ipc.on.ca/wp-content/uploads/2015/05/planning-for-success-pia-guide.pdf.

Table 9: The PIA process

Conceptual Analysis	Data Flow Analysis	Follow-up Analysis
Prepare a plain language description of the scope and business rationale of the proposed initiative. Identify in a preliminary way potential privacy issues and risks, and key stakeholders. Provide a detailed description of essential aspects of the proposal, including a policy analysis of major issues. Document the major flows of personal information. Compile an environment issues scan to review how other jurisdictions have handled a similar initiative. Identify stakeholder issues and concerns. Assess public reaction.	Analyse data flows through business process diagrams and identify specific personal data elements or clusters of data. Assess the proposal's compliance with freedom of information (FOI) and privacy legislation, and relevant programme statutes. Assess the proposal's broader conformity with general privacy principles. Analyse risk based on the privacy analysis of the initiative and identify possible solutions. Review design options and identify outstanding privacy issues/concerns that have not been addressed. Prepare a response for unresolved privacy issues.	Review and analyse the physical hardware and system design of the proposed initiative to ensure compliance with privacy design requirements. Provide a final review of the proposed initiative. Conduct a privacy and risk analysis of any new changes to the proposed initiative relating to hardware and software design to ensure compliance with FOI and privacy legislation, relevant programme statutes, and general privacy principles. Prepare a communications plan.

Source: Information and Privacy Commissioner of Ontario, Planning for Success: Privacy Impact Assessment Guide (2015) 5. https://www.ipc.on.ca/wp-content/uploads/2015/05/planning-for-success-pia-guide.pdf.

Assessment scope of PIA

A PIA is performed when:

1. Building a new information system that will hold and manage a large quantity of personal information;
2. Using a new technology where privacy can be violated;
3. Modifying an existing information system that holds and manages personal information; and
4. Collecting, using, keeping and/or destroying personal information during which a risk of privacy invasion can occur.

But it is not necessary to execute a PIA on all information systems. A PIA does not have to be performed when there is only a slight change of the existing program and system.

Examples of PIAs

PIA requirements in the United States of America

The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method of evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed.

PIA requirements in the European Union

The Regulation (EU) 2016/679 aka General Data Protection Regulation (GDPR) mandates data protection impact assessment (DPIA) in some cases. Aside from new IT systems and projects, the PIA approach has value for structured, periodic reviews or audits of an organization's privacy arrangements.

Table 10 lists PIA systems in three countries.

Table 10. Examples of national PIAs

	The United States of America	Canada	Australia/New Zealand
Legal ground	Section 208 of e-Government Act in 2002 OMB provides PIA requirements in OMB-M-03-22	Introduced its PIA policy and guideline in May 2002 Compulsory execution of PIA on the basis of common law on privacy	Voluntarily conduct of PIA (no legal ground) PIA Handbook for supporting PIA (2004, New Zealand), guideline for PIA (2004, Australia)

Subject	All executive branch departments and agencies and contractors who use IT or who operate websites for purposes of interacting with the public; relevant cross-agency initiatives, including those that further e-government	All programmes and services that government agencies provide	No duty or limit
Actor	Agencies performing e-government project dealing with personal information	Government agencies developing or operating the programmes and services	Relevant agencies or by requesting external consulting agencies
Publication	Making the PIA publicly available through the website of the agency, publication in the Federal Register, or other means, that may be modified or waived for security reasons, or to protect classified, sensitive or private information contained in an assessment Agencies shall provide the Director of OMB with a copy of the PIA for each system for which funding is requested	Making PIA summaries publicly available Providing a copy of the final PIA and report to the Office of the Privacy Commissioner in advance in order to get the proper advice or guidance with respect to proper protection strategy	The result of the PIA is usually not available publicly (no duty to report and publish)

Test Yourself

1. How is personal information different from other kinds of information?
2. Why should personal information be protected?
3. What is the significance of the OECD and United Nations principles on privacy protection?
4. Why is privacy impact assessment conducted?

6. CSIRT Establishment and Operation

This section aims to:

- Explain how to establish and operate a national Computer Security Incident Response Team (CSIRT); and
- Provide models of CSIRT from various countries

Cybercrime and various threats to information security need to be taken seriously because of their huge economic impact. Group-IB, a Russian security company, forecasted that the global cybercrime market would be USD 2.5 billion and grow to over USD 7 billion. According to IDC's research survey, almost half of the companies of all sizes reported that the "total" impact of financial loss per event was over USD 100,000, while 8.5 per cent of the companies reported financial loss of over USD 1 million.

Establishing a CSIRT is an effective way of mitigating and minimizing damage from attacks on information systems and breaches of information security.

6.1. Development and Operation of a CSIRT

A CSIRT is an organization, formalized as such or ad-hoc, that is responsible for receiving, reviewing and responding to computer security incident reports and activities. The basic purpose of a CSIRT is to provide computer security incident handling services to minimize the damage and allow efficient recovery from a computer security incident.[63]

In 1988, the first outbreak of a worm named Morris occurred and it spread rapidly around the world. After this, the Defence Advanced Research Projects Agency founded the Software Engineering Institute and then established the CERT/CC at Carnegie Mellon University under a contract from the Government of the United States of America. Since then, each country in Europe has established similar organizations. Since no single CSIRT has been able to solve broad vulnerability incidents, the Forum of Incident Response and Security Teams (FIRST) was established in 1990. Through FIRST, many information security agencies and CSIRTs are able to exchange opinions and share information.

Choosing the right CSIRT model[64]

There are five general organizational models for CSIRTs. The model that is most appropriate to an organization—i.e. considering various conditions such as the environment, financial status and human resources—should be adopted.

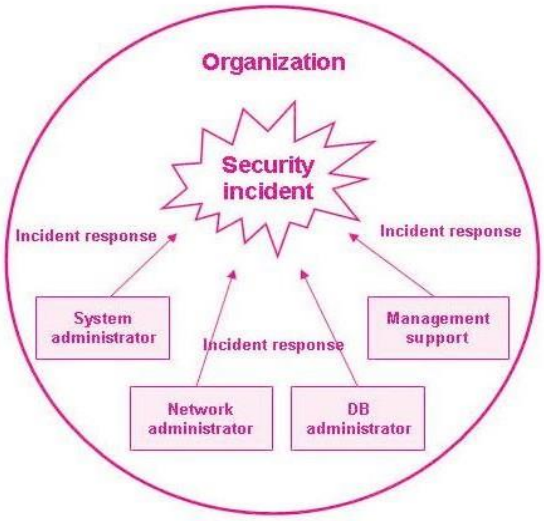
1. **Security team model (using existing IT staff)**

[63] Carnegie Mellon University. (2017, January 18). CSIRT Frequently Asked Questions (FAQ). https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485652.

[64] Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). *Organizational Models for Computer Security Incident Response Teams (CSIRTs)*. Software Engineering Institute. Retrieved from 10.1184/R1/6575921.v1

The security team model is not a typical CSIRT model. In fact, it is the opposite of a typical CSIRT. In this model, there is no centralized organization that is given responsibility for handling computer security incidents. Instead, incident handling tasks are conducted by system and network administrators, or by other security system specialists.

Table 10: Security team model



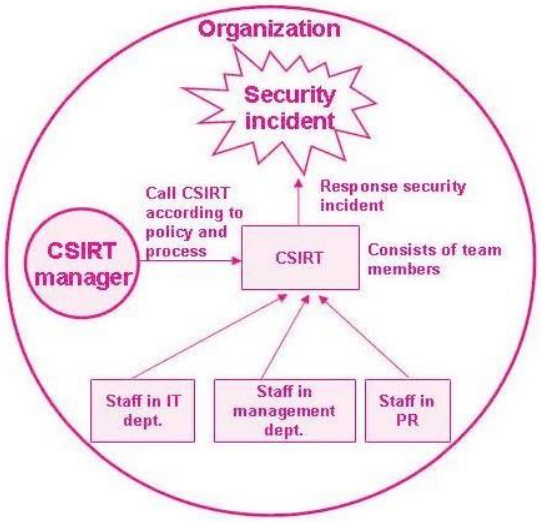
2. Internal distributed CSIRT model

This model is also referred to as the “distributed CSIRT”. The team in this model is composed of the CSIRT administrator who is responsible for reporting and overall management, and staff from other divisions of the concerned enterprise/agency. The CSIRT in this model is an officially recognized organization with the responsibility for handling all incident response activities. As the team is built within a company or an agency, the team is considered “internal”.

The internal distributed CSIRT model differs from the security team model in the following ways:

- The existence of more formalized incident handling policies, procedures and processes;
- An established method of communication with the whole enterprise concerning security threats and response strategies; and
- A designated CSIRT manager and team members who are specifically assigned incident handling tasks

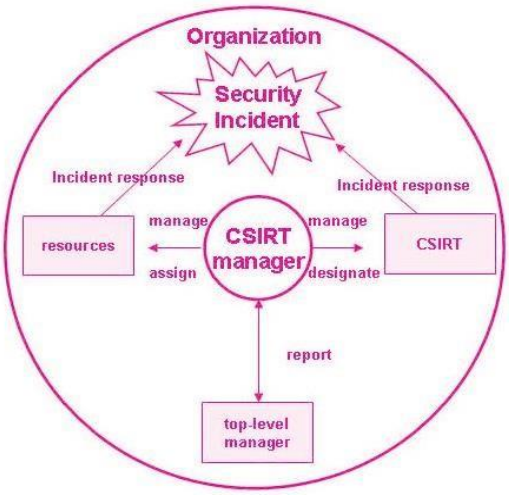
Figure 17: Internal distributed CSIRT model



3. Internal centralized CSIRT model

In the internal centralized CSIRT model, a centrally located team controls and supports the organization. The CSIRT has overall responsibility for all incident reporting, analysis and response. Thus, the team members cannot handle other jobs and spend all of their time working for the team and handling all incidents. Also, the CSIRT manager reports to high-level management such as the Chief Information Officer, Chief Security Officer or Chief Risk Officer.

Figure 18: Internal centralized CSIRT model

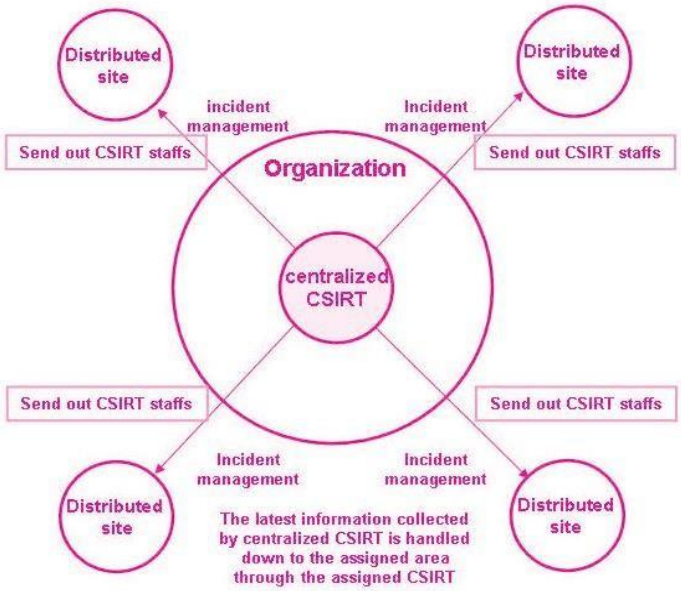


4. Combined distributed and centralized CSIRT model

This is also known as the “combined CSIRT”. Where a centralized CSIRT cannot control and support the entire organization, some team members are distributed among the organization’s sites/branches/divisions to provide within their areas of responsibility the same level of services as provided by the centralized CSIRT.

The centralized team provides high-level data analysis, recovery methods and mitigation strategies. It also furnishes the distributed team members with incident, vulnerability and artifact response support. The distributed team members at each site implement the strategies and provide expertise in their areas.

Figure 19: Combined CSIRT



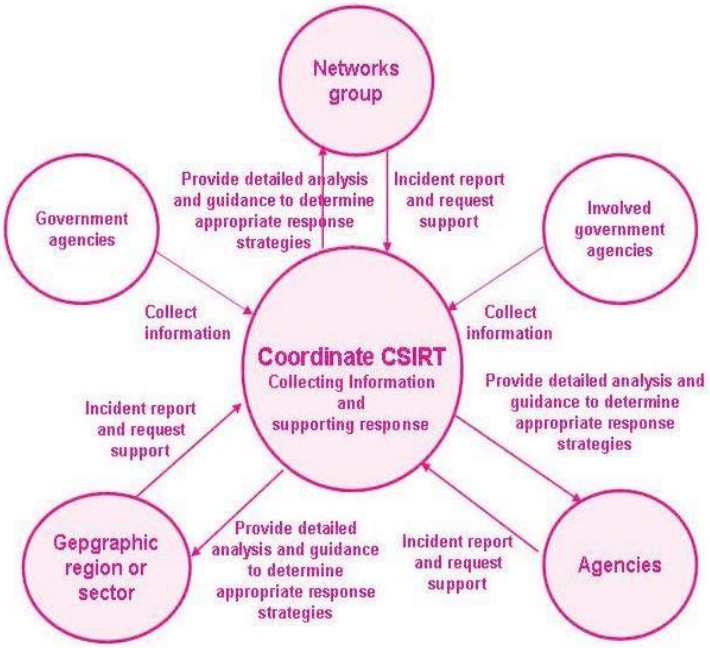
5. Coordinating CSIRT model

A coordinating CSIRT strengthens the function of the distributed teams in the combined CSIRT. In the coordinating CSIRT model, the team members in the combined CSIRT are grouped into independent CSIRTs based on such characteristics as network connectivity, geographical boundaries, and the like. They are controlled by the centralized CSIRT.

The coordinating CSIRT model is appropriate for a national CSIRT system. This model can be applied to the internal activities in an organization and to support and closely coordinate external agencies.

The coordination and facilitation activities cover information sharing, providing mitigation strategies, incident response, recovery method, research/analyses of trends and patterns of incident activity, vulnerability databases, clearinghouses for security tools, and advisory and alert services.

Figure 20: Coordinating CSIRT



Setting up a CSIRT: Steps for creating a national CSIRT[65]

There are five stages in setting up a CSIRT. The purpose, vision or roles of the CSIRT should serve as a guide in progression through the stages.

Stage 1 – Educating stakeholders about the development of a national team

Stage 1 is the awareness stage, where stakeholders develop understanding of what is involved in establishing the CSIRT. Through various education methods, they learn about:

a. The business drivers and motivators behind the need for a national CSIRT
b. Requirements for developing the incident response capabilities of a national CSIRT
c. Identifying the people to be involved in the discussions for building a national team
d. The key resources and critical infrastructure that exist within the country
e. The types of communications channels that need to be defined for communicating with the CSIRT constituency
f. Specific laws, regulations and other policies that will affect the development of the national CSIRT
g. Funding strategies that can be used to develop, plan, implement and operate the response capability
h. Technology and network information infrastructure that will be needed to support the operations of the national team
i. Basic response plans and interdependencies as they apply across a variety of sectors
j. The potential set of core services that a national CSIRT may provide to its constituency

[65] Killcrece, G. (2004). Steps for Creating National CSIRTs. Software Engineering Institute. Retrieved from https://resources.sei.cmu.edu/asset_files/WhitePaper/2004_019_001_53064.pdf

k. Best practices and guides

Stage 2 – Planning the CSIRT: Building on the knowledge and information gained during Stage 1

Stage 2 involves planning the CSIRT based on knowledge and information gained during Stage1. Issues discussed in Stage 1 are reviewed and discussed further, and then the precise details are determined and applied to the implementation plan. The plan is established considering the following activities:

a. Identifying the requirements and need for the national CSIRT —
   - Laws and regulations that will affect the operations of the national team
   - Critical resources that need to be identified and protected
   - Current incidents and trends that are being reported or should be reported
   - Existing incident response capabilities and computer security expertise
b. Defining the vision of the national CSIRT
c. Defining the mission of the national team
d. Determining the constituency (or constituencies) that it will serve
e. Identifying the communication interfaces between the constituency and the national team
f. Identifying the type of national (government) approval, leadership and sponsorship
g. Identifying the types of staff skills and knowledge that is needed to operate the team
h. Defining the types of roles and responsibilities for the national CSIRT
i. Specifying the incident management processes of the CSIRT as well as determining the relationships to similar processes in any of the external constituent organizations
j. Developing a standardized set of criteria and consistent terminology for categorizing and defining incident activity and events
k. Defining how the national CSIRT will interact with the constituency and other global CSIRTs or external partners
l. Determining any processes required for integration with existing disaster recovery, incident response plans, business continuity plans, crisis management or other emergency management plans
m. Developing project timelines
n. Creating the national CSIRT plan based on outcomes from the planning activity, vision and corresponding framework

Stage 3 – Implementing the CSIRT

In Stage 3, the project team uses the information and plan from Stages 1 and 2 to implement the CSIRT. The implementation process is as follows:

a. Getting the funds from sources identified during the planning stage
b. Announcing broadly that a national CSIRT is being created and where additional information can be obtained (about progress on the development, reporting requirements, etc.)
c. Formalizing coordination and communication mechanisms with stakeholders and other appropriate contacts

d. Implementing the secure information systems and network infrastructure to operate the national CSIRT (e.g., secure servers, applications, telecommunications equipment and other infrastructure support resources)
e. Developing the operation and process for the CSIRT staff, including the agreed standard in the planning stage and reporting guideline
f. Developing internal policies and procedures for access and operation of CSIRT equipment and personal equipment, as well as acceptable use policies
g. Implementing processes for the national CSIRT's interactions with its constituency
h. Identifying and hiring (or reassigning) personnel, obtaining appropriate training and education for the CSIRT staff, as well as determining other potential outreach efforts to train and educate the constituency

Stage 4 – Operating the CSIRT

At the operational stage, the basic services that the national CSIRT has to provide are defined and the operational efficiency to utilize an incident management capability is evaluated. Based on the results, operational details are established and improved. The activities at this stage are:

a. Actively performing the various services provided by the national CSIRT
b. Developing and implementing a mechanism for evaluating the effectiveness of the national CSIRT operations
c. Improving the national CSIRT according to the results of the evaluation
d. Expanding the mission, services and staff as appropriate and as can be sustained to enhance service to the constituency
e. Continuing to develop and enhance CSIRT policies and procedures

Stage 5 – Collaboration

A national CSIRT can develop a trusted relationship with key stakeholders through efficient operations (Stage 4). But a national CSIRT also needs to exchange important information and experiences of incident handling through long-term exchanges with cooperating institutions, domestic CSIRTs and international CSIRTs. The activities at this stage include:

a. Participating in data and information sharing activities and supporting the development of standards for data and information sharing between partners, other CSIRTs, constituents and other computer security experts
b. Participating in global "watch and warning" functions to support the community of CSIRTs
c. Improving the quality of CSIRT activities by providing training, workshops and conferences that discuss attack trends and response strategies
d. Collaborating with others in the community to develop best practice documents and guidelines
e. Reviewing and revising the processes for incident management as part of an ongoing improvement process

CSIRT services[66]

The services that CSIRTs provide may be classified into reactive services, proactive services and service quality management services.

Reactive services are the core services of a CSIRT. They include:

1. **Alerts and warnings** – This service includes providing information and response methods for dealing with problems such as a security vulnerability, an intrusion alert, a computer virus or a hoax.

2. **Incident handling** – This involves receiving, triaging and responding to requests and reports, and analysing and prioritizing incidents and events. Specific response activities include the following:

    - **Incident analysis** – An examination of all available information and supporting evidence or artifacts related to an incident or event. The purpose of the analysis is to identify the scope of the incident, the extent of damage caused by the incident, the nature of the incident and available response strategies or workarounds.

    - **Forensic evidence collection** – The collection, preservation, documentation and analysis of evidence from a compromised computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise.

    - **Tracking or tracing** – Involves tracking or tracing how the intruder entered the affected systems and related networks. This activity includes tracing the origins of an intruder or identifying systems to which the intruder had access.

3. **Incident response on site** – The CSIRT provides direct, on-site assistance to help constituents recover from an incident.

4. **Incident response support** – The CSIRT assists and guides the victim(s) of the attack in recovering from an incident via phone, e-mail, fax or documentation.

5. **Incident response coordination** – The response effort among parties involved in the incident is coordinated. This usually includes the victim of the attack, other sites involved in the attack and any sites requiring assistance in the analysis of the attack. It may also include the parties that provide IT support to the victim, such as ISPs and other CSIRTs.

6. **Vulnerability handling** – This involves receiving information and reports about hardware and software vulnerabilities, analysing the effects of the vulnerabilities, and developing response strategies for detecting and repairing the vulnerabilities.

    - **Vulnerability analysis** – Refers to technical analysis and examination of vulnerabilities in hardware or software. The analysis may include reviewing the source code, using a

[66] CERT. (2002). CSIRT Services. Software Engineering Institute. Retrieved from https://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_53048.pdf

debugger to determine where the vulnerability occurs, or trying to reproduce the problem on a test system.

- **Vulnerability response** – Involves determining the appropriate response to mitigate or repair vulnerabilities. This service can include performing the response by installing patches, fixes or workarounds. It also involves notifying others of the mitigation strategies, advisories or alerts.

- **Vulnerability response coordination** – The CSIRT notifies the various parts of the enterprise or constituency about the vulnerability and shares information about how to fix or mitigate it. The CSIRT also classifies successful vulnerability response strategies. Activities include analysing vulnerability or vulnerability reports and synthesizing technical analyses done by different parties. This service can also include maintaining a public or private archive or knowledge base of vulnerability information and corresponding response strategies.

7. **Artifact handling** – This includes analysis, response, coordination and handling of artifacts that involve computer viruses, Trojan horse programs, worms, exploit scripts and toolkits.

    - Artifact analysis – The CSIRT performs a technical examination and analysis of any artifact found in a system.

    - Artifact response – Involves determining the appropriate actions to detect and remove artifacts from a system.

    - Artifact response coordination – Involves sharing and synthesizing analysis results and response strategies pertaining to an artifact with other researchers, CSIRTs, vendors and other security experts.

Proactive services are for improving the infrastructure and security processes of the constituency before any incident or event occurs or is detected. They include the following:

1. **Announcements** – These include intrusion alerts, vulnerability warnings, security advisories, and the like. Such announcements inform constituents about new developments with medium- to long-term impact, such as newly found vulnerabilities or intruder tools. Announcements enable constituents to protect their systems and networks against just discovered problems before they can be exploited.

2. **Technology watch** – This involves monitoring and observing new technical developments, intruder activities and related trends to help identify future threats. The outcome of this service might be some types of guidelines, or recommendations focusing on more medium- to long-term security issues.

3. **Security audits or assessments** – This service provides a detailed review and analysis of an organization's security infrastructure, based on the requirements defined by the organization or by other industry standards that apply.

4. **Configuration and maintenance of security tools, applications, infrastructures and services** – This service provides appropriate guidance on how to securely configure and maintain tools, applications and the general computing infrastructure.

5. **Development of security tools** – This service includes the development of new, constituent- specific tools, software, plug-ins and patches that are developed and distributed for security.

6. **Intrusion detection services** – CSIRTs that perform this service review existing IDS logs, analyse them and initiate a response for events that meet their defined threshold.

7. **Security-related information dissemination** – This service provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security.

Security quality management services are designed to provide knowledge gained from responding to incidents, vulnerabilities and attacks synthetically. Such services include:

1. **Risk analysis** – This involves improving the CSIRT's ability to assess real threats, provide realistic qualitative and quantitative assessments of risks to information assets, and evaluate protection and response strategies.

2. **Business continuity and disaster recovery planning** – Business continuity and recovery from disaster caused by computer security attacks are ensured through adequate planning.

3. **Security consulting** – CSIRTs can also provide practical advice and guidance for business operations.

4. **Awareness building** – CSIRTs are able to improve security awareness by identifying and providing information and guidance about security practices and policies that constituents require.

5. **Education/Training** – This service involves providing education and training on such topics as incident reporting guidelines, appropriate response methods, incident response tools, incident prevention methods, and other information necessary to protect, detect, report and respond to computer security incidents. Training modalities include seminars, workshops, courses and tutorials.

6. **Product evaluation or certification** – The CSIRT may conduct product evaluations on tools, applications or other services to ensure the security of the products and their conformance to acceptable CSIRT or organizational security practices.

Table 11 shows the level of each CSIRT service—i.e. whether it is a core, additional or unusual service—in each CSIRT model.

Table 11: CSIRT services

Service Category	Services		Security Team	Distributed	Centralized	Combined	Coordinating
Reactive	Alerts and Warnings		Additional	Core	Core	Core	Core
	Incident Handling	Incident Analysis	Core	Core	Core	Core	Core
		Incident Response on Site	Core	Additional	Additional	Additional	Unusual
		Incident Response Support	Unusual	Core	Core	Core	Core
		Incident Response Coordination	Core	Core	Core	Core	Core
	Artifact Handling	Vulnerability Analysis	Additional	Additional	Additional	Additional	Additional
		Vulnerability Response	Core	Additional	Unusual	Additional	Additional
		Vulnerability Response Coordination	Additional	Core	Core	Core	Core
		Artifact Analysis	Additional	Additional	Additional	Additional	Additional
		Artifact Response	Core	Additional	Additional	Additional	Additional
		Artifact Response Coordination	Additional	Additional	Core	Core	Core
Proactive	Announcements		Unusual	Core	Core	Core	Core
	Technology Watch		Unusual	Additional	Core	Core	Core
	Security Audits or Assessments		Unusual	Additional	Additional	Additional	Additional
	Configuration and Maintenance of Security Tools, Applications, Infrastructures and Services		Core	Additional	Additional	Additional	Unusual
	Development of Security Tools		Additional	Additional	Additional	Additional	Additional
	Intrusion Detection Services		Core	Additional	Additional	Additional	Unusual
	Security-Related Information		Unusual	Additional	Core	Core	Core

	Dissemination					
Security Quality Management	Risk Analysis	Unusual	Additional	Additional	Additional	Additional
	Business Continuity and Disaster Recovery Planning	Unusual	Additional	Additional	Additional	Additional
	Security Consulting	Unusual	Additional	Additional	Additional	Additional
	Awareness Building	Unusual	Additional	Additional	Additional	Core
	Education/Training	Unusual	Additional	Additional	Additional	Core
	Product Evaluation or Certification	Unusual	Additional	Additional	Additional	Additional

Source:
Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). *Organizational Models for Computer Security Incident Response Teams (CSIRTs)*. Software Engineering Institute. Retrieved from 10.1184/R1/6575921.v1

6.2. International CSIRT Associations

Currently, there are a number of specialized international CSIRT associations established to respond to computer security incidents around the world. While national CSIRTs can respond to attacks and perform their other functions, a cross-border attack involving more than two economies requires the attention of an international CSIRT association.

Forum of Incident Response Security Teams[67]

The Forum of Incident Response Security Teams (FIRST) consists of CERTs, government agencies and security companies from 52 countries. Its membership includes 248 organizations, including CERT/CC and US-CERT (as of September 2011). FIRST is an association for information sharing and cooperation among incident response teams. Its goal is to activate incident response and protection activities and motivate cooperation among members by providing them with technology, knowledge and tools for incident response. The activities of FIRST are as follows:

- Developing and sharing best practices, procedure, tools, technical information and methodologies for incident response and protection;
- Motivating the development of policies, services and security products of good quality;
- Supporting and developing appropriate computer security guidelines;
- Helping governments, enterprises and educational institutions to establish an incident response team and expand it; and

[67] Forum of Incident Response and Security Teams, Inc. (2020). *About FIRST*. FIRST. http://www.first.org/about.

- Facilitating the sharing of technology, experiences and knowledge among members for a safer electronic environment

6.3. Regional CSIRT Associations

Asia-Pacific CERT[68]

The Asia-Pacific Computer Emergency Response Team (APCERT) was established in February 2003 to serve as a network of security experts, strengthen incident response and improve security awareness in the Asia-Pacific region. The first conference of Asia-Pacific CSIRTs was held in Japan in 2002. APCERT was founded a year later at a conference in Taipei attended by 14 Asia-Pacific CSIRTs. As of September 2011, APCERT has 18 full members and 9 general members from 18 economies.

APCERT members agree that today's computer security incidents are too numerous, complicated and difficult to control for any one organization or country, and that a more effective response can be deployed by collaborating with other members of APCERT. As in FIRST, the most important concept in APCERT is the relationship of trust between members for exchanging information and cooperating with each other. Thus, APCERT activities are designed to:

- Enhance Asia-Pacific regional and international cooperation;
- Jointly develop measures to deal with large-scale or regional network security incidents;
- Improve security information sharing and technology exchange, including information on computer viruses, exploit scripts, and the like;
- Improve collaborative research on common problems;
- Assist other CERTs in the region in responding effectively to computer security incidents; and
- Provide advice and solutions to legal issues related to regional information security and incident response

European Government CERT[69]

The European Government CERT (EGC) is a non-official committee that is associated with governmental CSIRTs in European countries. Its members include Finland, France, Germany, Hungary, the Netherlands, Norway, Sweden, Switzerland and the United Kingdom. Its roles and responsibilities are to:

- Jointly develop measures to deal with large-scale or regional network security incidents;
- Promote information sharing and technology exchange in regard to security incidents and malicious code threats and vulnerability;
- Identify areas of knowledge and expertise that could be shared within the group;

[68] Asia Pacific Computer Emergency Response Team. *Background*. Background : About APCERT . http://www.apcert.org/about/background/index.html.

[69] EGC Group. *EGC group*. European Government CERTs (EGC) group. http://www.egc-group.org/.

- Identify areas of collaborative research and development on subjects that are of interest to members; and
- Promote the formation of government CSIRTs in European countries

European Network and Information Security Agency[70]

The purpose of European Network and Information Security Agency (ENISA) is to enhance network security and information security in the European Union through the creation of a NIS culture. It was established in January 2004 by the Council of Ministers and the European Parliament to respond to “hi-tech” crime. It has the following roles:

- Providing support to ensure NIS among members of ENISA or the European Union;
- Promoting stable exchange of information between stakeholders; and
- Improving the coordination of functions relating to NIS.

ENISA is expected to contribute to international efforts to mitigate viruses and hacking and establish online monitoring of threats.

AfricaCERT

The purpose of the African forum of computer incident response teams, is to propose solution to challenges for internet health in Africa Internet Ecosystem. The objectives of AfricaCERT include

- Coordinating cooperation among CSIRTS;
- Assisting African countries in establishing CSIRTs by providing expertise and advise; and
- Fostering and supporting education and outreach programs in ICT Security in and among African countries.

6.4. National CSIRTs

Several countries have organized a national CSIRT. Table 12 lists the countries and their respective CSIRTs as well as the website for each.

Table 12: List of national CSIRTs

Country	Official name	Home pages
Abu Dhabi	Abu Dhabi Police Computer Emergency Response Team	https://adsic.abudhabi.ae

[70] ENISA. (2021, January 15). About ENISA - The European Union Agency for Cybersecurity. ENISA. http://www.enisa.europa.eu/about-enisa.

Argentina	ICIC-CERT	http://www.icic.gob.ar
Australia	Australia Computer Emergency Response Team	http://www.auscert.org.au
Australia	Australia Cyber Security Centre	http://www.cyber.gov.au
Austria	CERT.at	https://www.cert.at
Azerbaijan	CERT.AZ	http://www.cert.az
Bangladesh	Bangladesh e-Government Computer Incident Response Team	https://www.cirt.gov.bd
Brazil	Computer Emergency Response Team Brazil	http://www.cert.br
Brunei Darussalam	Brunei Computer Emergency Response Team	http://www.brucert.org.bn
Belarus	CERT.BY	http://cert.by
Belgium	Belgian Federal Cyber Emergency Team	http://www.cert.be
Bhutan	Bhutan Computer Incident Response Team	http://www.btcirt.bt
Bolivia	Cenro de Gestion de Incidentes Informaticos	https://cgii.gob.bo/
Brazil	Computer Emergency Response Team Brazil	http://www.cert.br
Brunei	Brunei Computer Emergency Response Team	http://www.brucert.org.bn
Canada	Canadian Centre for Cyber Security	http://www.cyber.gc.ca
Chile	Chilean Computer Emergency Response Team	http://www.clcert.cl
China	National Computer Network Emergency Response Technical Ream – Coordination Center of China	http://www.cert.org.cn
Croatia	CarNet CERT	http://www.carnet.hr

Czech Republic	CSIRT.CZ	http://www.clcert.cl
Denmark	Danish Computer Emergency Response Team	http://www.cert.dk
Egypt	Danish Computer Emergency Response Team	http://www.egcert.eg
Estonia	CERT-EE	https://ria.ee
Finland	National Cyber Security Centre Finland	http://www.ncsc.fi
France	CERT-FR	http://www.cert.ssi.gouv.fr
Germany	CERT-Bund	http://www.bsi.bund.de/certbund
Ghana	CERT-GH National Cyber Security Centre of Ghana	https://cybersecurity.gov.gh
Hong Kong, China	Hong Kong Computer Response Coordination Centre	http://www.hkcert.org
Hungary	CERT-Hungary National Cyber Security Center	https://nki.gov.hu
Iceland	CERT-IS Computer Incident Response Team Iceland	https://www.cert.is
India	CERT-In Indian Computer Emergency Response Team	http://www.cert-in.org.in
Indonesia	Indonesia Security Incident Response Team on Internet Infrastructure	http://www.idsirtii.or.id
Iran	CERT CC Maher	https://www.ircert.com
Italia	CSIRT Italia	https://www.csirt-ita.it/
Japan	JP CERT Coordination Center	http://www.jpcert.or.jp
Kazakhstan	Kazakhstan Computer Emergency Response	http://www.cert.kz

Macau	MOCERT	http://www.mocert.org
Lithuania	LITNET CERT	http://cert.litnet.lt
Malaysia	Malaysian Computer Emergency Response Team	http://www.mycert.org.my
Mexico	Universidad Nacional Autonoma de Mexico	http://www.cert.org.mx
Mongolia	Mongolian Cyber Emergency Response / Coordination Centre	http://www.mncert.org
Morocco	maCERT	
Netherlands	National Cyber Security Centre of The Netherlands	http://www.ncsc.nl
New Zealand	CERT NZ	http://www.cert.govt.nz
Nigeria	ngCERT Nigerian Computer Emergency Response Team	http://www.cert.gov.ng
Norway	Norwegian Computer Emergency Response Team	https://nsm.stat.no/norcert
Pakistan	PakCERT	http://www.pakcert.org
Papua New Guinea	PNGCERT	https://www.pngcert.org.pg
Philippines	Philippines Computer Emergency Response Team	http://www.phcert.org
Poland	Computer Emergency Response Team Polska	http://www.cert.pl
Portugal	CERT.PT	https://www.cncs.gov.pt
Qatar	Qatar National Center for Information Security	http://www.qcert.org
Republic of	CSIRT-IE	https://ncsc.gov.ie/csirt

Ireland		
Romania	Romanian National Computer Security Incident Response Team	http://cert.ro
Russia	RU-CERT Computer Security Incident Response Team	http://www.cert.ru
Saudi Arabia	Computer Emergency Response Team – Saudi Arabia	http://www.cert.gov.sa
Singapore	Singapore Computer Emergency Response Team	https://www.csa.gov.sg/singcert
Slovakia	SK-CERT	https://www.sk-cert.sk
Slovenia	Slovenia Computer Emergency Response Team	http://www.cert.si
Republic of Korea	CERT Coordination Center Korea	http://www.krcert.or.kr
Spain	INCIBE-CERT Spanish National Cybersecurity Institute - National CSIRT	https://www.incibe-cert.es
Sri Lanka	SL CERT | CC	http://www.cert.gov.lk
Sweden	CERT-SE	http://www.cert.se
Switzerland	Computer Emergency Response Team of the Swiss Government	http://www.melani.admin.ch
Taiwan Province of China	Taiwan Computer Emergency Response Team/Coordination Center	http://www.twcert.org.tw

Taiwan Province of China	Taiwan Computer Emergency Response Team/Coordination Center	http://www.twcert.org.tw
Tonga	CERT Tonga	http://www.cert.gov.to
Tunisia	TunCERT – Tunisian Computer Emergency Response Team	https://www.ansi.tn
Turkey	TP-CERT National Cyber Security Incident Response Team	http://www.uekae.tubitak.gov.tr
Ukraine	Computer Emergency Response Team of Ukraine	https://cert.gov.ua
United Arab Emirates	The United Arab Emirates Computer Emergency Response Team	http://www.aecert.ae
Uganda	CERT.UG Uganda Computer Emergency Response Team	http://www.ug-cert.ug
United Kingdom	National Cyber Security Centre	http://www.ncsc.gov.uk
United States of America	United States Computer Emergency Readiness Centre	https://www.us-cert.gov
Uzbekistan	Computer Emergency Response Team of Uzbekistan	http://uzcert.uz
Viet Nam	Viet Nam Computer Emergency Response Team	http://www.vncert.gov.vn

Something to Do

Is there a national CSIRT in your country?

1. If yes, describe it in terms of the model it is patterned after and how it works. Assess how effective it is in performing its functions.
2. If none, determine which CSIRT model would be appropriate for your country and describe what is required to establish a national CSIRT in your country.

Test Yourself

1. What are the key functions of CSIRTs?

2. How different are international CSIRTs from national CSIRTs?

3. What are the requirements for setting up a CSIRT?

7. Life Cycle of Information Security Policy

This section aims to:

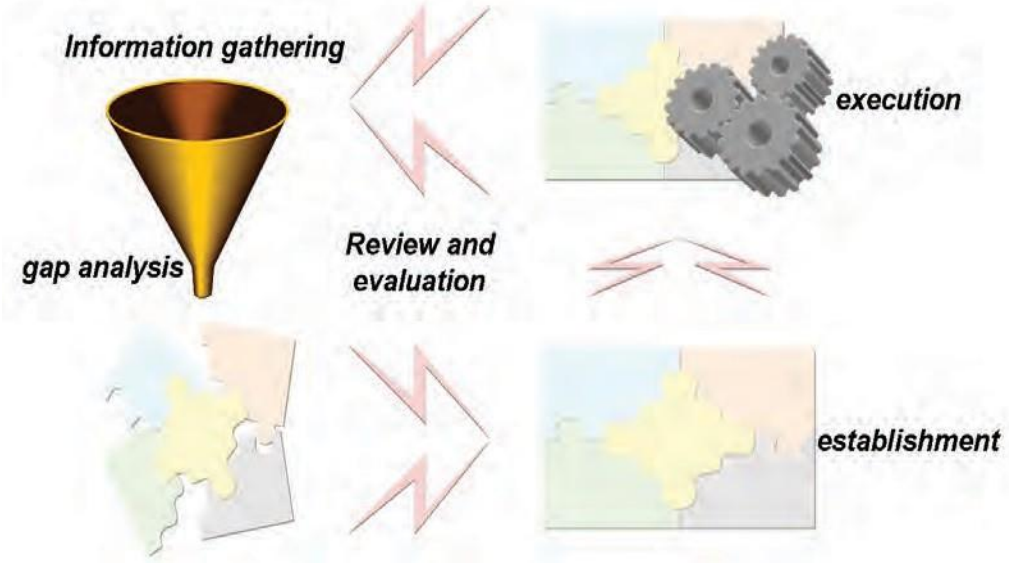
- Give an overview of the information security policymaking process; and
- Discuss issues that policymakers must consider in information security policymaking

Policymakers need to take into account a number of considerations, among them the rationale for a policy, available resources, the policy direction, budgetary and legal requirements, and expected policy outcomes. In this section, these considerations are discussed in the context of the different stages of information security policymaking.

It should be noted that different countries will have slightly different policy considerations and contexts. The policymaking process described in this section is generic and based on the assumption that there is no existing national information security policy.

As with other policies, the life cycle of information security policy can be divided into four phases: (1) information gathering and gap analysis; (2) establishment of the policy; (3) implementation of the policy; and (4) control and feedback (see figure 22). In addition, a national information security policy should include the information security strategy, legal relationships, information security organization, information security technology, and the interrelationships among them.

Figure 21: Life cycle of information security policy



7.1. Information Gathering and Gap Analysis

The first phase in formulating an information security policy is information gathering and gap analysis.

In information gathering, it is useful to review examples of information security and related policies from other countries, as well as related policies within the country itself.

In gap analysis, it is important to understand the existing infrastructure related to information security, such as existing laws and systems, as well as areas or gaps that need to be filled. This is an important step as it determines the direction or priority of the information security policy to be established.

Information gathering

Gathering cases from overseas: In locating relevant cases in other countries, policymakers should consider similarities in the —

- Level of national information security
- Direction of policy establishment
- Network and system infrastructure

Considering these similarities, the following materials should be collected —

- Information on the establishment and operation of organizations engaged in information security (see sections 3 and 6 of this module)
- Information security policies, laws and regulations (see section 3)
- Internationally used information security methodology and examples from different countries (see section 4)
- Threat trends and countermeasures or controls according to attack types (see sections 2 and 6)
- Countermeasures for privacy protection (see section 5)

Gathering domestic materials: Although most policymakers are not experts in information security, they perform activities that are related or relevant to information security. Specifically, they craft laws, regulations and policies in areas related to information security. However, because laws, regulations and policies tend to focus on specific areas, the correlation among them might not be immediately apparent to policymakers. Thus, there is a need to collect and analyse and evaluate all laws, regulations and policies that are related or relevant to information security.

Gap analysis

Sun Tzu's *The Art of War* says, "Know your enemy." This means you should know your limits as well as that of your enemy. In the case of information security policymaking, this would mean knowing what needs to be protected through an information security policy as well as vulnerabilities and threats to information security.

Gap analysis can be divided into two phases:

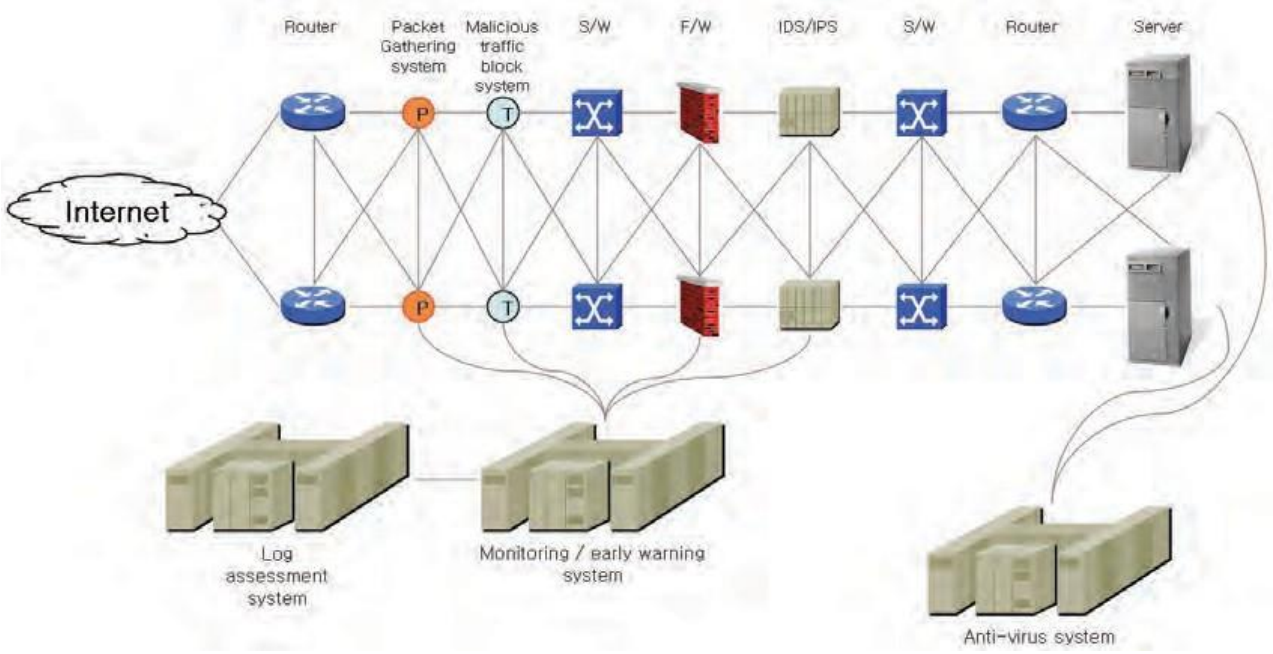
1. Understanding the country's abilities and capacities—i.e. the organization and human resources, as well as the information and communication infrastructure—in the general area of information security; and
2. Identifying the external threats to information security

Policymakers need to be familiar with the information security organization and human resources, that is public and private institutions in areas related to information security. They should know the organizations involved in information security related work and understand their scope of work, roles and responsibilities. This is important in order not to duplicate existing structures for information security.

It is also at this point that experts in information security should be identified and tapped. Such experts typically have a background in law, policy, technology, education and related fields.

The information-communication infrastructure refers to the IT structure that collects, processes, stores, searches, transmits and receives electronic control management systems and information. In short, this is the information system and network. Understanding the current status of the information-communication infrastructure is particularly important from an economic point of view. Because large investments are needed to connect the whole country, making the most of existing information-communication facilities is advantageous. Figure 23 shows a sample information-communication infrastructure for information security. It does not include all items that may be required and is given here only for illustrative purposes. Note the relationship among the various components of the network.

Figure 22: Sample network and system structure



Policymakers need to be able to grasp how the general network and systems for information security are set up.

The second step in gap analysis is to identify the external threats to information security. As mentioned in section 2, threats to important information are not only increasing but also becoming more sophisticated. Policymakers need to understand these threats to be able to decide what countermeasures are necessary. In particular, policymakers must understand:

- The penetration rate of threats to information security
- The most common and current attack types
- Threat types and their expected degree of strength in the future

After analysing national organizations, human resources and the information-communication infrastructure, as well as grasping the threat components in the area of information security, it is important to derive the vulnerable components. This is determining the extent to which the country can resist the external threat components. This determination can be made by examining the following:

- Current status of the CERT and its ability to react
- Current status of experts on information security
- Construction level and intensity of the information security system
- Legal protection against information asset infringement
- Physical environment for protecting information assets

The objective of gap analysis is to be able to identify the practical countermeasures that need to be taken. It should be emphasized that it is the most basic step in information security policymaking.

7.2. Formulating Information Security Policy

Formulating a national information security policy involves: (1) setting the policy direction; (2) constituting the information security organization and defining its roles and responsibilities; (3) articulating the information security policy framework; (4) instituting and/or revising laws to make them consistent with the policy; and (5) allocating a budget for information policy implementation.

1. Setting the policy direction and pushing ahead

In most cases, the pursuit of information security policy should be spearheaded by the government rather than left to the private sector. In particular, the government needs to set the policy, play a lead role in putting the necessary infrastructure in place and provide long-term support. The private sector joins the project in time, principally to take part in research and development, and system construction.

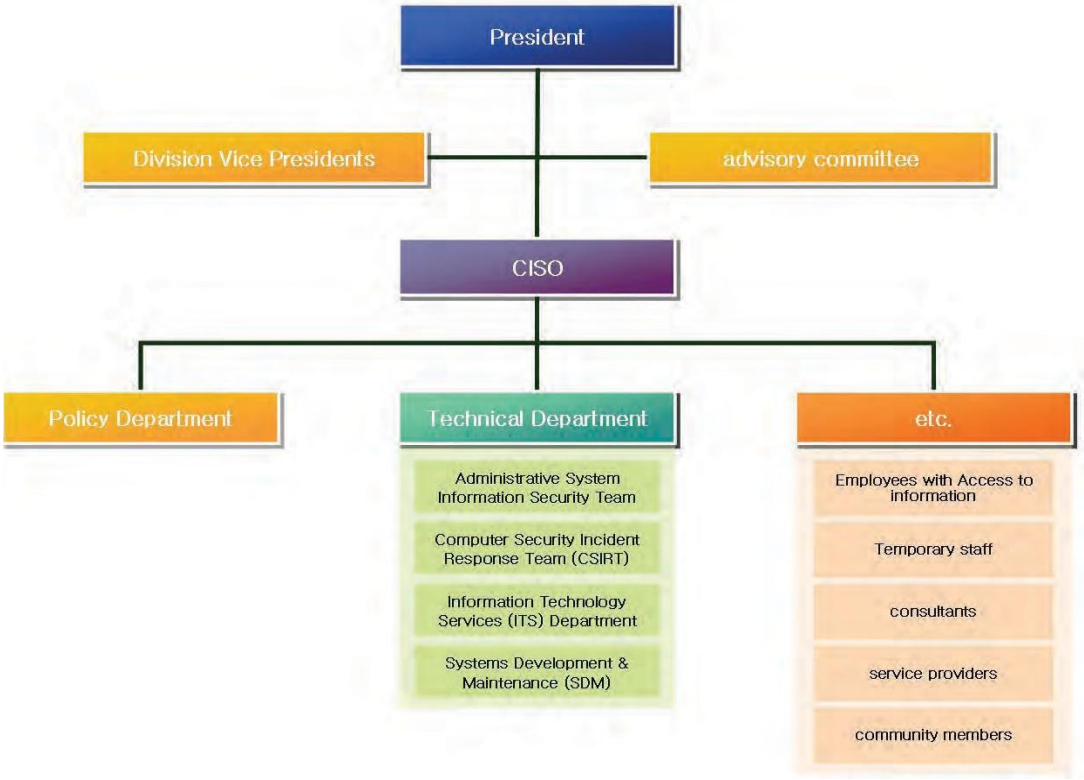
Planning for private sector participation includes awareness-raising activities alongside building and strengthening the information-communication infrastructure. If the government aims to

encourage the private sector to accept the information security strategy, then government should play a supportive rather than a controlling role. This includes distributing information security guidelines.

2. Constitution of the information security organization, and definition of roles and responsibilities[71]

Once the direction for information security policy has been set, the implementing organization should be constituted. Figure 24 shows the structure of a generic national information security organization.

Figure 23: A generic national information security organization



National information security organizations differ slightly according to the characteristics and cultures of each country. However, a basic principle is to ensure that roles and responsibilities are clearly delineated.

Administrative organization

Division Vice-Presidents have primary responsibility for information collected, maintained and/or identified as utilized or "owned" by their respective divisions. They may designate an

[71] Sinclair Community College. *Information Security Organization – Roles and Responsibilities*. Information Security Policy. https://it.sinclair.edu/index.cfm/services/student-and-guests-services/policies-and-security-information/information-security-policy/.

Information Security Officer and other individuals to assist the Information Security Officer in implementing the information security policy. These designated staff must ensure that information assets within their span of control have designated owners, that risk assessments are conducted and that mitigation processes based on those risks are implemented.

Supervisors (Directors, Chairs, Managers, etc.) manage employees with access to information and information systems and specify, implement and enforce the information security controls applicable to their respective areas. They must ensure that all employees understand their individual responsibilities with regards to information security and that employees have the access required to perform their jobs. Supervisors should periodically review all users' access levels to ensure that they are appropriate and take appropriate action to correct discrepancies or deficiencies.

The Chief Information Security Officer (CISO) is responsible for coordinating and overseeing the information security policy. Working closely with various divisions, the CISO may recommend that supervisors of specific divisions designate other representatives to oversee and coordinate particular elements of the policy. The CISO also assists information owners with information security best practices in:

- Establishing and disseminating enforceable rules regarding access to and acceptable use of information resources;
- Conducting/Coordinating information security risk assessment and analysis;
- Establishing reasonable security guidelines and measures to protect data and systems;
- Assisting with monitoring and management of systems security vulnerabilities;
- Conducting/Coordinating information security audits; and
- Assisting with investigations/resolution of problems and/or alleged violations of national information security policies.

Technical organization

The Administrative System Information Security Team develops and implements measures to ensure that administrative application security controls allow stakeholders appropriate access to information while meeting national legal and ethical obligations to protect private, sensitive and critical information. The team develops processes and standards to provide optimal availability, integrity and confidentiality of administrative system information, including processes for users to request initial access and access changes; documentation of authorized user access, as well as user/supervisor rights and responsibilities; and resolution of security-related conflicts and issues.

The team includes the Division Information Security Officers and the CISO. The team is advised by the Department Information Security Officers and Administrative Systems Administrators.

The **CSIRT** provides information and assists stakeholders in implementing proactive measures to reduce the risks of computer security incidents, and in investigating, responding to and minimizing damage from such incidents when they occur. The CSIRT also determines and recommends follow-up actions. The two-layer CSIRT is composed of an operational team charged with initial identification, response, triage and determination of escalation requirements, and a management team charged with spearheading the national response to

major or significant incidents. The CISO and delegated IT staff members from IT Services and Systems Development and Maintenance are part of the operational CSIRT. The CSIRT management team is composed of the Chief Information Officer, Chief of Police, Director of Public Information, Director of IT Services, Director of Systems Development and Maintenance, CISO, systems and network manager, a legal advisor, a human resources advisor, and delegates with technical expertise specifically appointed by the Vice Presidents.

IT Services Department staff members include systems and network administrators and engineers, and technical services providers such as the IT Help Desk, user support technicians and voice communications administrators. They are responsible for the integration of technical information security tools, controls and practices in the network environment. They receive reports of suspected information security failure or incidents from end-users.

Systems Development and Maintenance staff members include developers and database administrators. They develop, practice, integrate and implement security best practices for national applications, and train Web application developers in the use of application security principles.

Others

Employees with access to information and information systems must comply with applicable national policies and procedures, as well as any additional practices or procedures established by their unit heads or directors. This includes protecting their account passwords and reporting suspected misuse of information or information security incidents to the appropriate party (usually their supervisor).

Temporary staff members are considered employees and have the same responsibilities as regular full- or part-time employees with access to information and information systems.

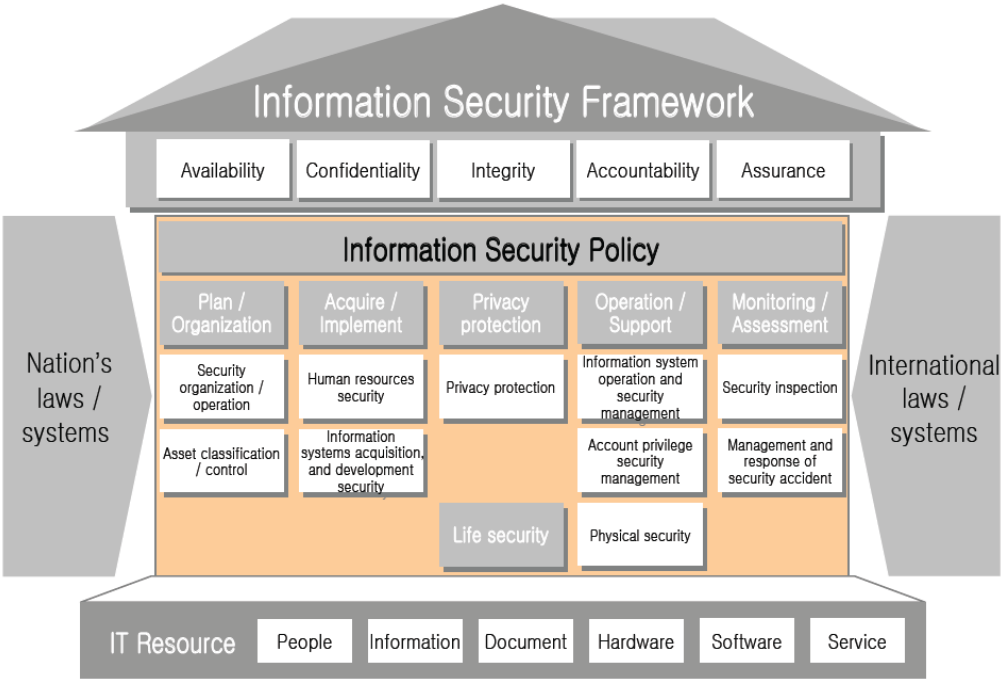
Consultants, service providers and other contracted third parties are granted access to information on a “need-to-know” basis. A network account required by a third party must be requested by a “sponsor” within the organization who shall ensure that the third-party user understands the individual responsibilities related to the network account, and approved by the appropriate vice-president or director. The user must keep his/her password(s) secure and be accountable for any activity resulting from the use of his/her user ID(s) within reasonable scope of his/her control.

3. Setting the framework of information security policy

Information security framework

The information security framework sets the parameters for information security policy. It ensures that the policy takes into account IT resources (people, information documents, hardware, software, services); reflects international laws and regulations; and meets the principles of information availability, confidentiality, integrity, accountability and assurance. Figure 24 shows an information security framework.

Figure 24: Information security framework



The information security policy is the most important part of the information security framework. The policy includes five areas, discussed below.

a. Plan and Organization: This area includes security of organization and operation, and asset classification and control.

Security organization and operation covers the —

- Organization and system of the national information security organization
- Procedure of each information security organization
- Constitution and management of the nation's information security
- Cooperation with the relevant international agency
- Cooperation with an expert group

Asset classification and control includes —

- Ownership grant and classification standard for important information assets
- Registration instruction and risk assessment of important information assets
- Management of access privileges over important information assets
- Publication and export of important information assets
- Important information assets revaluation and exhaustion
- Security management of documents

b. **Acquisition and Implementation**: This area includes human resources security, and information systems acquisition and development security.

   Human resources security involves defining a management method for hiring new employees that includes —

   - Human resources security countermeasure and security training
   - Processing of breach of security regulation and the law
   - Security management of third party access
   - Security management of access of outsourcing personnel
   - Work and management of third parties and outsourcing employees
   - Security management of computer room and equipment
   - Access to main facilities and buildings
   - Processing of security accidents

   Information systems acquisition and development security requires —

   - Security checks when an information system is acquired
   - Security management for in-house and outsourcing of application programs
   - A national encryption system (encrypt program and key, and so on)
   - Tests after program development
   - Suggested security requirements when outsourcing development
   - Security verification with development and acquisition

c. **Privacy Protection**: The inclusion of privacy protection in an information security policy is not mandatory. However, including it is an advantage because privacy protection is an international issue. Privacy protection provisions should cover the following —

   - Personal information collection and use
   - Prior consent when taking advantage of people's privacy
   - PIA

d. **Operation and Support**: This area has to do with physical and technical security. Use of the network and system is regulated in detail, and the physical security of the information and communication infrastructure is defined.

   Information system operation and security management involves defining the following —

   - Operation and security management of the server, network, application and database
   - Development of the information security system
   - Log and back-up against legal action
   - Information storage management
   - Mobile computing
   - Standard for custody and security of computer data

- Electronic commerce services

Account privilege security management – Access control and account management have to be defined to guarantee confidentiality in the use of the nation's information depository. This includes —

- Registration, deletion, privilege management of users of the national information system
- Account and privilege management of encrypted networking

Physical security – Physical security refers to protecting information and communication facilities that keep important information. It includes —

- Configuring and managing security area methods
- Access and transport control for the computer centre
- Prevention of damage from natural and other disasters

e. Monitoring and Assessment: This area of information security policy requires the formulation of standards and processes for preventing security incidents and managing and responding to security incidents.

Security inspection includes —

- Establishing a security inspection plan
- Implementing periodic security inspection
- Formulating/Organizing report forms
- Identifying the subject of security inspections and report targets

Management of and response to *security* incident requires defining —

- The work and role of each organization in processing security incidents
- Procedures for observing and recognizing symptoms of security incidents
- Security incident processing procedure and response method
- Measures to be undertaken after security incident processing

4. Instituting and/or revising laws to be consistent with the information security policy

Laws must be consistent with the information security policy. There should be laws governing State organizations and private enterprise. Tables 13 to 15 list laws related to information security in Japan, the European Union and the United States of America respectively. In Japan, the representative IT law is the Basic Act on the Formation of an Advanced Information and Telecommunications Network Society. This law is the fundamental standard for information security in the country and all related laws need to conform to it.

Table 13: Information security related laws in Japan

Laws	Target industry	Target of regulation	Penalty
Unauthorized Computer Access Law	All industry	Action that promotes unauthorized access and supplies another person's ID information without notice	
Act on the Protection of Personal Information	Private enterprises that use private information for business purposes	Privacy information (address, phone number, e-mail, and so on) management	Criminal liability, fine
Act on Electronic Signatures and		Facilitation of electronic commerce that takes advantage of the Internet and	

Table 14: Information security related laws in the European Union

Law	Details
A Common Regulatory Framework (Directive 2002/21/ EC)	• Presents the framework for regulating telecommunication networks and services • Aims to protect privacy through secure communication networks
EU Directive on Data Protection (Directive 1995/46/ EC)	• Guideline on processing and free removal of private information • Fundamental law defining member nations' responsibility and recognizing the ultimate authority of individuals over private information • More stringent than the United States of America's standard

EU Directive on Electronic Signatures (Directive 1999/93/EC) EU Directive on Electronic Commerce	• Governs use of electronic signatures • Regulates the conduct of electronic commerce
Cybercrime Treaty	• Most comprehensive international treaty about cybercrime • Defines in detail all criminal acts that use the Internet and their corresponding penalties
Data Preservation Guideline on Communication and Networks	• Requires communication service providers to preserve call data from six months to 24 months (promulgated following the terrorist attacks in Madrid and London in 2004 and 2005 respectively)

Table 15: Information security related laws in the United States of America

Laws	Target industry	Target of	Penalty
Federal Information Security Management Act of 2002	Federal administrative agencies	Information of administrative agencies, IT system, information security	-
Health Insurance Privacy and Accountability Act of 1996	Medical institutions and medical service providers	Electronic data of personal medical information	Criminal liability, fine
Gramm-Leach-Bliley Act of 1999	Financial institutions	Privacy information of customers	Criminal liability, fine
Sarbanes-Oxley Act of 2002	Listed companies on The United States of America's Stock Exchange	Internal control and public financial record	Criminal liability, fine

California Database Security Breach Information Act of 2003	Administrative agencies and private enterprise in California	Encrypted privacy information	Fine and notification to victim

5. Allocating a budget for information policy implementation

Implementation of a policy requires a budget. Table 16 shows the budget for information security in United Kingdom and the United States of America in recent years.

Table 16: Information security budget of the United Kingdom and the United States of America

(Units: United Kingdom – million pounds; United States of America – million dollars)

United Kingdom	**2016**	**2017**	**2018**	**2019**	**2020**
Information security budget	1, 092	1, 137	-	-	-
United States of America	**2016**	**2017**	**2018**	**2019**	**2020**
Total annual IT budget	-	81, 495	137, 489	-	-
Information security budget	-	13, 150	14, 980	16, 650	17, 430
Percentage of total IT budget	-	16.13	10.89	9.10	-

Sources: Statista.co for United Kingdom & United States of America figures.

Something To Do

If your country has an information security policy, trace its development in terms of the five aspects of information security policy formulation described above. That is, describe the:

1. Policy direction
2. Information security organization
3. Policy framework
4. Laws supporting information security policy
5. Budgetary allocation for information security

If your country does not yet have an information security policy, outline some possibilities for each of the five aspects above towards the formulation of the policy. Use the following questions as a guide:

1. What should be the direction of information security policy in your country?

2. What organizational set-up should be in place? Which organizations should be involved in information security policy development and implementation in your country?

3. What specific issues should the policy framework address?

4. What laws should be enacted and/or repealed in support of the information policy?

5. What budgetary considerations should be taken into account? Where should the budget be drawn from?

Training participants from the same country can do this activity together.

7.3. Policy Execution / Implementation

The smooth implementation of information security policy requires cooperation among government, private and international agents. Figure 25 shows specific areas of information policy implementation where cooperation is crucial.

Figure 25: Areas for cooperation in information security policy implementation

Information security policy development

Table 17 presents how the government, private sector and international organizations can contribute to national information security policy development.

Table 17: Cooperation in information security policy development (example)

Sector	Contributions to Policy Development
Government	• National strategy and planning organization: ensure match between information policy and the national plan • ICT organization: ensure the cooperation of the nation's information security technology standard establishment • Information security trend analysis organization: reflect domestic and international security trend and analysis in policy • Legal analysis organization: check match between information security policy and existing laws • National information organization: cooperate in direction setting and strategy establishment • Investigative agencies: cooperate in the processing of security accidents
Private sector	• Information security consulting companies: use of professional agents in information security policymaking • Private information security technology laboratory: establish technology standards related to information security • Information security department of universities and/or graduate schools: provide expertise in policy formulation
International organizations	• Ensure compliance with international policy standards • Coordinate the response to international threats and accidents

Information and communication infrastructure management and protection

Effective use (collection, custody, etc.) of information requires the proper administration and protection of the IT infrastructure. A good information security policy is useless in the absence of a sound IT infrastructure.

The effective management and protection of information and communication infrastructure requires cooperation among the network, system and IT area managers. It also benefits from cooperation between public and private institutions (see table 18).

Table 18: Cooperation in administration and protection of information

Sector	Contributions to Administration and Protection of Information and Communication Infrastructure
Government sector	• Information and communication network related organization: define composition and level of security of the national information and communication network • ICT laboratory: distribute public standards and adopt usable technology
Private sector	• ISP: cooperate in the composition of the national information and communication network • ICT laboratory: provide technical development services and cooperate in the operation of a stable information and communication infrastructure and security technology
International organizations	• Cooperate with the international technology standard organization for international information and communication, and for securing new IT

Prevention of and response to threats and incidents

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

Table 19: Cooperation in information security accident response (example)

Sector	Contributions
Government organizations	• Security incident response organization: provide situational analysis, hacking incident response, and technology to respond to violations and accidents • National information organization: analyse and inspect information security related violations and accidents • Investigative agencies: cooperate with the organization involved in apprehending and prosecuting offenders • Organization providing security evaluation: verify the safety and reliability of information network and information security-based production • Information security education organization: analyse the causes of information security accidents and educate people to prevent the recurrence of accidents
Private groups	• Private incident response organization: provide response and technical support • Private investigative agencies: cooperate with national investigative agencies
International organizations	• In cases of international threats and incidents, report to and cooperate with Interpol, CERT/CC

Prevention of information security incidents

Preventing information security violations and accidents includes monitoring, education and change management. The national CSIRT is the main monitoring organization. A critical area is matching information policy and real monitoring data. Thus, it is necessary to discuss the scope of information policy monitoring. Moreover, it is important to educate government and private sector employees, as well as the general public, about information security policy. It may be necessary to change certain attitudes towards information and behaviors that impact on security information. Information security education and change management are defined in the US SP 800-16 (Information Technology Security Training Requirements).

Table 20: Cooperation in information security violation and accident prevention (example)

Sector	Coordination
Government organizations	• Monitoring agent: continuous monitoring of the network and advanced detection of security threats • Collecting agent: information sharing with international organizations and security sites • Training institute: periodic simulation training to develop the ability and capacity to respond quickly to information security violations and accidents
Private organizations	• ISP, security control and anti-virus company: provide traffic statistics, information on attack type and profile of worms/viruses
International organizations	• Provide information on the attack type, profile of worms/viruses, and the like

Privacy security

Cooperation is needed to establish Internet privacy protection measures, private locational information incident prevention, protection of private biological information and reporting of violations of privacy.

Table 21: Coordination in privacy protection (example)

Sector	Coordination
Government agencies	• System analysis organization: conduct business related to private locational information, and analysis of trends in internal and external personal information protection • Planning organization: improve laws/systems, technical/ administrative measures and standards management • Technical support: coordinate cyber-user certification for businesses • Service organizations: coordinate support for troubleshooting privacy violations and spam
Private organizations	• Personal information security organization: register requirements and organize cooperative associations for personal information security

International organizations	• Cooperate to apply international personal information security standards

International coordination

Information security cannot be achieved through the efforts of one country alone because information security violations tend to be international in scope. Thus, international coordination in information security protection, both in government and in the private sector, must be institutionalized.

For the private sector, the relevant international organization for the promotion and protection of information security is CERT/CC. Among governments, ENISA (for the European Union) and the ITU aim to foster cooperation in information security among countries.

In each country, there must be a government institution whose role is to facilitate cooperation by both government and private organizations with international agencies and institutions.

7.4. Review and Evaluation of Information Security Policy

The final step in information security policymaking is evaluating policy and supplementing underdeveloped areas. Policy revision is essential after the efficiency of an information security policy has been determined.

A domestic policy evaluation method can be implemented to determine the efficiency of the national information security policy. Aspects of this method are discussed below.

Use of audit organizations

There are organizations whose role is to conduct appraisals and evaluation of policy. Such an organization should conduct regular audits of the national information security policy. Moreover, this organization should be independent of the information security policymaking organization and the implementing organization.

Revising information security policy

Problem areas are usually identified during the policy audit. There should be a process for revising the policy to address these problem areas.

Changes in the environment

It is important to react sensitively to changes in the policy environment. Changes arising from international threats (attacks) and vulnerabilities, changes in the IT infrastructure, grade changes of critical information, and other such important changes should be immediately reflected in the national information security policy.

Something to Do

Identify the government agencies and private organizations in your country that would need to collaborate and cooperate in the implementation of a national information security policy. Identify the international organizations that they need to coordinate with as well.

Training participants from the same country can do this activity together.

References

(ISC)². (2020). *Cybersecurity Certification: CISSP - Certified Information Systems Security Professional: (ISC)²*. Cybersecurity Certification| CISSP - Certified Information Systems Security Professional | (ISC)². http://www.isc2.org/cissp.

Asia Pacific Computer Emergency Response Team. *Background*. Background: About APCERT. http://www.apcert.org/about/background/index.html.

Carnegie Mellon University. (2017, January 18). CSIRT Frequently Asked Questions (FAQ). https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485652.

Carnegie Mellon University. *Software Engineering Institute*. The CERT Division. https://www.sei.cmu.edu/about/divisions/cert/index.cfm.

CERT. (2002). *CSIRT Services*. Software Engineering Institute. Retrieved from https://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_53048.pdf

Commission of the European Communities, A European Programme for Critical Infrastructure Protection (2006). Brussels, Belgium. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.

Commission of the European Communities, A strategy for a Secure Information Society – “Dialogue, partnership and empowerment” (2006). Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0251&qid=1612332935197&from=EN.

Commission of the European Communities, Critical Information Infrastructure Protection: "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (2009). Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009DC0149&qid=1612333230526&from=EN.

Commitment to a Free,Fair and Secure Cyberspace. NISC. (2018). https://www.nisc.go.jp/eng/.

Common Criteria. (2009). (publication). *Common Criteria for Information Technology Security Evaluation*. Retrieved from https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf

Common Criteria. Common Criteria: New CC Portal. http://www.commoncriteriaportal.org/.

Council of Europe action against Cybercrime. Council of Europe. https://www.coe.int/en/web/portal/coe-action-against-cybercrime.

Council of the European Union, Council Conclusions on the Digital Agenda for Europe (2010). Brussels, Belgium. https://data.consilium.europa.eu/doc/document/ST-10130-2010-INIT/en/pdf.

Council of the European Union, Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security (2009). Belgium, Brussels. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF.

Cross, D. (2017, January 10). *World's Most Recent & Biggest Hacking Incidents*. Web Hosting Media. https://webhostingmedia.net/recent-biggest-hacking-incidents.

Denning, D. E., Arquilla, J., & Ronfeldt, D. (2001). Activism, Hacktivism, And Cyberterrorism: The Internet As A Tool For Influencing Foreign Policy. In *Networks and Netwars. The Future of Terror, Crime, and Militancy* (pp. 239–288). essay, RAND Corporation.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (1995). *Official Journal of the European Communities*, *38*(281), 31–50. https://doi.org/https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

EGC Group. *EGC group*. European Government CERTs (EGC) group. http://www.egc-group.org/.

Egede, I. (2018, July 31). *Threat Hunting for File Hashes as an IOC*. Infosec Resources. https://resources.infosecinstitute.com/topic/threat-hunting-for-file-hashes-as-an-ioc.

ENISA. (2021, January 15). *About ENISA - The European Union Agency for Cybersecurity*. ENISA. http://www.enisa.europa.eu/about-enisa.

EUR-Lex, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504.

European Commission, A Digital Agenda for Europe (2010). Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245&qid=1612333676302&from=EN.

European Commission, Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision (2010). Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010PC0517&qid=1612334410667&from=EN.

European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 460/2004 establishing the European Network and

Information Security Agency as regards its duration (2010). Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010PC0520&qid=1612335155929&from=EN.

European Commission, Proposal For A Regulation Of The European Parliament And Of The Council Concerning The European Network And Information Security Agency (ENISA) (2010). Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010PC0521&qid=1612334562226&from=EN.

European Council, Conclusions of the European Council (25/26 March 2010) (2010). Brussels, Belgium. https://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ec/113591.pdf.

Forum of Incident Response and Security Teams, Inc. (2020). *About FIRST*. FIRST. http://www.first.org/about.

Gillis, A. S. (2020, February 12). *What is an Intrusion Prevention System (IPS)?* SearchSecurity. https://searchsecurity.techtarget.com/definition/intrusion-prevention.

HM Government. (2016). (rep.). *National Cyber Security Strategy 2016-2021*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Information and Privacy Commissioner of Ontario, Planning for Success: Privacy Impact Assessment Guide (2015). https://www.ipc.on.ca/wp-content/uploads/2015/05/planning-for-success-pia-guide.pdf.

International Telecommunication Union. ICT Security Standards Roadmap. http://www.itu.int/ITU-T/studygroups/com17/ict/index.html.

International Telecommunications Union. (2006). World Summit on the Information Society: About WSIS. http://www.itu.int/wsis/basic/about.html.

International Telecommunications Union. (2021). ITU Cybersecurity Activities. http://www.itu.int/en/action/cybersecurity/Pages/default.aspx.

International Telecommunications Union. (2021). *ITU-D Cybersecurity*. ITU-D. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx.

International Telecommunications Union. *SG17 - Study Group Structure (Study Period 2017-2020)*. ITU. http://www.itu.int/net4/ITU-T/lists/sgstructure.aspx?Group=17&Period=16.

International Telecommunications Union. Study Group 17 at a glance. http://www.itu.int/net/ITU-T/info/sg17.aspx.

Internet Governance Forum. (2021). http://www.intgovforum.org/.

ISMS Accreditation Centre. *Overview of the ISMS conformity assessment scheme*. ISMS-AC. https://isms.jp/english/isms/about.html.

ITU-D ICT Applications and Cybersecurity Division. (2009). ITU National Cybersecurity/CIIP Self-Assessment Tool. http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

Killcrece, G. (2004). *Steps for Creating National CSIRTs*. Software Engineering Institute. Retrieved from https://resources.sei.cmu.edu/asset_files/WhitePaper/2004_019_001_53064.pdf

Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). *Organizational Models for Computer Security Incident Response Teams (CSIRTs)*. Software Engineering Institute. Retrieved from 10.1184/R1/6575921.v1

Korolov, M. (2019, June 27). *What is a botnet? When armies of infected IoT devices attack*. CSO Online. https://www.csoonline.com/article/3240364/what-is-a-botnet.html.

Kotadia, M. (2005, April 5). *E-mail worm graduates to IM*. ZDNet. https://www.zdnet.com/article/e-mail-worm-graduates-to-im/.

OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 9–17 (2013). Paris, France. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

OECD, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002). Paris, France. https://www.oecd.org/digital/ieconomy/15582260.pdf.

OECD. (2006, May). OECD Working Party on Information Security and Privacy WPISP. Paris.

https://www.gpdp.it/documents/10160/10704/Working+Party+on+Information+Security+and+Privacy.pdf/586b9ff2-0ae8-4cb1-873a-2025fb6f5a15?version=1.1

Organisation for Economic Co-operation and Development. *Privacy Online: OECD Guidance on Policy and Practice*. OECD. https://www.oecd.org/digital/ieconomy/privacyonlineoecdguidanceonpolicyandpractice.htm.

Permanent Stakeholders' Group. (P. Dorey & S. Perry, Eds.), The PSG Vision for ENISA (2006). https://www.enisa.europa. eu/about-enisa/structure-organization/psg/files/psg-vision.

Ramasubramanian, S., & Shaw, R. (2007, September). ITU Botnet Mitigation Project: Background & Approach. International Telecommunication Union. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit.pdf

Ramasubramanian, S., Ansari, S., & Purcell, F. (2005). Governing Internet Use: Spam, Cybercrime and e-Commerce. In D. Butt (Ed.), *Internet governance: Asia-Pacific*

Perspectives (pp. 89–104). essay, APDIP. https://www.unapcict.org/sites/default/files/2019-01/Internet%20Governance%20-%20Asia-Pacific%20perspectives.pdf.

Rosencrance, L. (2020, August 27). *What is advanced persistent threat?* SearchSecurity. https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT.

SecureAuth. (2017, July 14). secureauth_ciam_infographic_170714.pdf. Irvine.

Shimeall, T. J., & Williams, P. (2002). Models of information security trend analysis. *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Defense and Law Enforcement*. https://doi.org/10.1117/12.479291

Sinclair Community College. *Information Security Organization – Roles and Responsibilities*. Information Security Policy. https://it.sinclair.edu/index.cfm/services/student-and-guests-services/policies-and-security-information/information-security-policy/.

Stack, B. (2017, December 6). *Here's How Much Your Personal Information Is Selling for on the Dark Web*. Experian. https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

Tan, D. R. (1999). Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United Stats and European Union. *Loyola of Los Angeles International and Comparative Law Review*, *21*(4). https://digitalcommons.lmu.edu/ilr/vol21/iss4/5.

Telecommunications and Information. Asia-Pacific Economic Cooperation. (2020, April). https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.

U.S. Government Printing Office. (2014). *An Act to Provide for an Ongoing, Voluntary Public-Private Partnership to Improve Cybersecurity, and to Strengthen Cybersecurity Research and Development, Workforce Development and Education, and Public Awareness and Preparedness, and for Other Purposes*.

UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files (1990). https://www.refworld.org/docid/3ddcafaac.html.

Adopted by General Assembly resolution 45/95 of 14 December 1990. Contain procedures for implementing regulations concerning computerized personal data files.

The White House. (2003). (rep.). *The National Strategy to Secure Cyberspace*. Retrieved from https://www.hsdl.org/?view&did=1040

The White House. (2018). (rep.). *National Cyber Strategy of the United States of America*. Retrieved from https://www.defense.gov/Explore/News/Article/Article/1641969/white-house-releases-first-national-cyber-strategy-in-15-years/

Wikimedia Foundation. (2020, December 31). *Zero-day (computing)*. Wikipedia. https://en.wikipedia.org/wiki/Zero-day_(computing).

Wikimedia Foundation. (2021, February 1). *Antivirus software*. Wikipedia. http://en.wikipedia.org/wiki/Antivirus_software.

WSIS, WSIS: Plan of Action (2003). International Telecommunications Union. https://www.itu.int/net/wsis/docs/geneva/official/poa.html.

APCICT/ESCAP

The Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT) is a regional institute of the Economic and Social Commission for Asia and the Pacific (ESCAP). APCICT aims to strengthen the efforts of the member countries of ESCAP to use ICT in their socioeconomic development through human and institutional capacity-building. APCICT's work is focused on three pillars: training, knowledge-sharing, and multi-stakeholder dialogue and partnership. Together they form an integrated approach to ICT human capacity building.

APCICT is located at Incheon, Republic of Korea.

http://www.unapcict.org

ESCAP

The Economic and Social Commission for Asia and Pacific (ESCAP) is the regional development arm of the United Nations and serves as the main economic and social development centre for the United Nations in Asia and the Pacific. Its mandate is to foster cooperation between its 53 members and 9 associate members. ESCAP provides the strategic link between global and country-level programmes and issues. It supports Governments of countries in the region in consolidating regional positions and advocates regional approaches to meeting the region's unique socioeconomic challenges in a globalizing world.

The ESCAP office is located at Bangkok, Thailand.

http://www.unescap.org

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

Asian and Pacific Training Centre for Information and Communication Technology for Development
5th Floor, G-Tower, 175 Art Center Daero, Yeonsu-gu, Incheon, Republic of Korea

www.unapcict.org