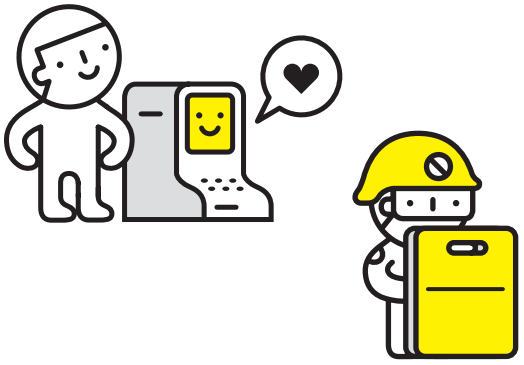
CYBER SECURITY ISSUE

Anatomy of Cybercrime

Things that the developing nations should consider



The introduction of Information and Communication Technologies (ICTs) into many aspects of everyday life has led to the development of the modern concept of the Information Society. This development of the Information Society offers great opportunities for supporting democracy and improvement in daily life through online banking, shopping, etc. However, the growth of the Information Society is accompanied by new and serious threats. Essential services such as water and electricity supply now rely on ICTs. Cars, traffic control, elevators, air conditioning and telephones also depend on the smooth functioning of ICTs. Attacks against information infrastructure and Internet services now have the potential to harm society in new and critical ways.

The attacks against information infrastructure and Internet services have already taken place. Online fraud, the dissemination of child pornography and hacking attacks are just some examples of computer-related crimes that are committed on a large scale every day. The financial damage caused by cybercrime is enormous. By some estimates, revenues from cybercrime exceeded USD 100 billion in 2007, outstripping the illegal trade in drugs for the first time. Nearly 60 per cent of businesses in the United States believe that cybercrime is more costly to them than physical crime. These estimates clearly demonstrate the importance of protecting information infrastructure.

A. What is "cybercrime"?

Most reports, guides or publications on cybercrime begin by defining the term "cybercrime." One common definition describes cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity. Some definitions try to take the objectives or intentions into account and define cybercrime more precisely, defining cybercrime as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks."

B. Why is it important to the developing nations?

Finding response strategies and solutions to the threat of cybercrime is a major challenge, especially for developing countries. A comprehensive Anti-Cybercrime Strategy generally contains technical protection measures, as well as legal instruments. The development and implementation of these instruments need time. Technical protection measures are especially cost-intensive. Developing countries need to integrate protection

measures into the roll-out of the Internet from the beginning. Although this might initially raise the cost of Internet services, the long-term gains in avoiding the costs and damage inflicted by cybercrime are large and far outweigh any initial outlays on technical protection measures and network safeguards. Developing countries need to bring their anti-cybercrime strategies into line with international standards from the outset.

The risks associated with weak protection measures could in fact affect developing countries more intensely, due to their less strict safeguards and protection. The ability to protect customers, as well as firms, is a fundamental requirement not only for regular businesses, but also for online or Internet-based businesses. In the absence of Internet security, developing countries could encounter significant difficulties promoting e-business and participating in online service industries.

C. How to prepare strategies for anti-cybercrime?

Since cybercrimes can pose threat beyond the national border and requires international cooperation, the fight against cybercrime has become an essential element of law enforcement activities worldwide. Due to rapid development of ICTs, especially in developing countries, the creation and implementation of an effective anti-cybercrime strategy as part of a national cybersecurity strategy is essential.

➔Cybercrime legislation as an integral part of a cybersecurity strategy

The International Telecommunication Union (ITU) Global Cybersecurity Agenda (GCA) is a global framework for dialogue and international cooperation to coordinate the international response to the growing challenges to cybersecurity and to enhance confidence and security in the information society. GCA highlights all required measures relevant to any cybersecurity strategy in five pillars.

➔Relevance of cybercrime issues within five pillars of cybersecurity

The GCA has seven main strategic goals, built on five work areas: 1) legal measures; 2)technical and procedural measures; 3)organizational structures; 4)capacity building; 5)international cooperation.

1) Legal measures Within the five pillars, the legal measures are probably the most relevant with regard to criminalize acts such as computer fraud, illegal access, data interference, copyright violations and child pornography. Additionally, it is essential to prepare the necessary tools and instruments to investigate cybercrime by development of the legal national framework to be able to cooperate with law enforcement agencies abroad.

2) Technical and procedural measures Cybercrime-related investigations very often have a strong technical component. Also, it involves precise procedures in order to maintain the integrity of the evidence during an investigation. Improving technical protection by implementing proper security standards is another important step. Technical protection should be essential to end-users, businesses, service providers, and software companies. Logistically, it is easier to focus on protection of core infrastructure, but as the number of network users increases day by day, the protection of end-user infrastructure is vital for the whole network's technical protection. With regard to Internet service providers and product vendors, they can operate as a guarantor of security activities on the grounds that they contact with clients directly by distributing of protection tools and information on the current status of most recent scams.

3) Organizational structures An effective fight against cybercrime requires highly developed organizational structures. This is due to avoid losses caused by overlapped investigations and to have clear competence for carrying out complex investigations that require the assistance of different legal and technical experts.

4) Capacity building Both developed and developing countries require capacity building in order to effectively investigate based on ensured global standards. Furthermore, user education is also needed. Certain cybercrimes such as phising and spoofing take place owing to lack of awareness by victims. Users can be educated through public campaigns, lessons in schools, libraries, ICT centers and universities, and public private partnerships. Even though states are reluctant to emphasize the threats rising in online communication services, it is very significant to let citizens and clients to know about the open communication of the latest cybercrime threats.

5) International cooperation In a large number of cases data transfer processes in the Internet affect more than one country. Therefore, it is obligatory to think about international cooperation in order to establish cybercrime strategies.

➔Implementation of existing strategies

Developing countries can adopt existing strategies of industrialized countries as an alternative. This could surely reduce the cost and time for development of its own cybersecurity strategies. However, the implementation of an existing anti-cybercrime strategy poses a number of difficulties. Because there is a gap between resources and capabilities of each country, it might not be the optimal solutions to the developing countries. Also, developing countries need to take into account the matter of compatibility of respective legal system; status of supporting initiatives such as education of the society; extent of self-protection measures in place; and extent of private sector support through public-private partnerships.

➔Consideration of regional differences

Given the international nature of cybercrime, the harmonization of national laws and techniques is vital in the fight against cybercrime. However, harmonization must consider regional demand and capacity.

Imagining a safer online society in the future

Due to the transnational nature of the Internet, it is in particular important to collaborate with other countries and to set a fundamental legal framework to regulate the violations against the fair use of the Internet. Developing countries exceptionally, have to establish the protection measures even though this mission will be somewhat difficult considering that the nations possess relatively poor resources. The benefits obtained from completing the mission will reach by far beyond the cost they spent. As a consequence, regardless of the amount of resources and capabilities, it is recommended for developing nations to be conducive to create safer online society on the whole by arranging anti-cybercrime measures. ICWT

About the Article

This article is a brief summary of *Understanding Cybercrime: A Guide for Developing Countries* published by International Telecommunication Union (ITU) in 2009. This article is prepared to provide insight for developing countries about cybercrimes with descriptions of cybercrimes categorized into five sections as well as ITU's anti-cybercrime strategies.

Better know about cybercrime

1. Offences against the Confidentiality, Integrity and Availability of Computer Data and Systems	
Illegal Access (Hacking, Cracking)	"Hacking" refers to unlawful access to a computer system, one of oldest computer-related crimes. Famous targets of hacking attacks include the United States National Aeronautics and Space Administration (NASA), the United States Airforce, Pentagon, Yahoo, Google, ebay and the German Government. Examples of hacking offences include breaking the password of password-protected Websites and circumventing password protection on a computer.
Data Espionage	Sensitive information is often stored in computer systems. If the computer system is connected to the Internet, offenders can try to access this information via the Internet from almost any place in the world. In the 1980s, a number of German hackers succeeded in entering United States government and military computer systems, obtained secret information and sold this information to agents from the Soviet Union.
Illegal Interception	Offenders can intercept communications between users or intercept data transfers when users upload data onto Web servers or access Web-based external storage media to record the information exchanged.
Data Interference	Lack of access to data can result in considerable (financial) damage. Offenders can violate the integrity of data and interfere with them by deleting, suppressing, and/or altering data, and/or restricting access to them.
System Interference	The same concerns over attacks against computer data apply to attacks against computer systems. Attacks can be carried out by physical attacks on the computer system. If offenders are able to access the computer system, they can destroy hardware. For highly profitable e-commerce businesses, the financial damages caused by attacks to the computer system are often far greater than the mere cost of computer hardware.
2. Content-related Offences	
Erotic or Pornographic Material (excluding Child Pornography)	Sexually-related content was among the first content to be commercially distributed over the Internet, which offers advantages to retailers of erotic and pornographic material including: exchange of media without the need for cost-intensive shipping; worldwide access, reaching a significantly larger number of customers than retail shops; anonymity in that consumers of pornography appreciate, in view of prevailing social opinions.
Child Pornography	International organizations are engaged in the fight against online child pornography, with several international legal initiatives including: the 1989 United Nations Convention on the Rights of the Child, the 2003 European Union Council Framework Decision on combating the sexual exploitation of children and child pornography, and the 2007 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, among others.
Racism, Hate Speech, Glorification of Violence	Recently, the number of Websites offering racist content and hate speech has risen. A study in 2005 suggested a rise of 25 per cent in the number of Websites promoting racial hatred, violence and xenophobia between 2004 and 2005. In 2006, over 6,000 such Websites existed on the Internet.

Religious Offences	A growing 271 of Websites present material that is in some countries covered by provisions related to religious offences e.g., anti-religious written statements. Although some material documents reflect facts and trends, this information may be considered illegal in some jurisdictions.
Illegal Gambling and Online Games	Internet games and gambling are one of the fastest growing areas in the Internet. Linden Labs, the developer of the online game Second Life, reports that some ten million accounts have been registered. Reports show that some games have been used to commit crimes including: exchange and presentation of child pornography, fraud, gambling in online casinos and libel (e.g. leaving slanderous or libelous messages).
Libel and False Information	Websites can present false or defamatory information, especially in forums and chat rooms, where users can post messages without verification by moderators. Minors are increasingly using Web forums and social networking sites where such information can be posted as well. Criminal behavior can include the publication of intimate photographs or false information about sexual behaviors.
Spam and Related Threats	"Spam" describes the emission of unsolicited bulk messages. Although various types of spam exist, the most common one is e-mail spam. Offenders send out millions of e-mails to users, often containing advertisements for products and services, but frequently also malicious software. Since the first spam e-mail was sent in 1978, the tide of spam e-mails has increased dramatically. Today, e-mail provider organizations report that as many as 85 to 90 per cent of all e-mails are spam.

3. Copyright and Trademark-related Offences

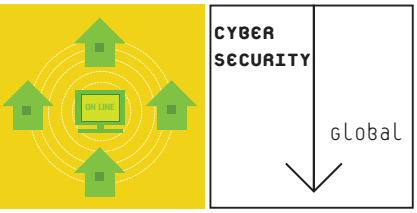
Copyright-related Offences	The basis for current copyright violations is fast and accurate reproduction. Before digitalization, copying a record or a video-tape always resulted in a degree of loss of quality. Today, it is possible to duplicate digital sources without loss of quality, and also, as a result, to make copies from any copy. The most common copyright violations include: exchange of copyright-protected songs, files and software in file-sharing systems; and the circumvention of Digital Rights Management systems.
Trademark-related Offences	Trademark violations are similar to copyright violations, a well-known aspect of global trade. Violations related to trademarks have transferred to cyberspace, with varying degrees of criminalization under different national penal codes. The most serious offences include: The use of trademarks in criminal activities with the aim of misleading targets, and domain or name-related offences.

4. Computer-related Offences

Computer-related Fraud	Computer-related fraud is one of the most popular crimes on the Internet, as it enables the offender to use automation and software tools to mask criminals' identities. Online Auction Fraud and Advance Fee Fraud fall in this category.
Computer-related Forgery	Computer-related forgery describes the manipulation of digital documents by creating a document that appears to originate from a reliable institution; manipulating electronic images (for example, pictures used as evidence in court); or altering text documents.
Identity Theft	The term identity theft – that is neither consistently defined nor consistently used – describes the criminal act of fraudulently obtaining and using another person's identity. These acts can be carried out without the help of technical means as well as online by using Internet technology.
Misuse of Devices	Cybercrime can be committed using only fairly basic equipment. Offences such as libel or online fraud need nothing more than a computer and Internet access and can be carried out from a public Internet café. More sophisticated offences can be committed using specialized software tools.

5. Combination Offence

Cyber-terrorism	Back in the 1990s, the discussion about the use of the network by terrorist organizations was focusing on network-based attacks against critical infrastructure such as transportation and energy supply "cyber terrorism" and the use of information technology in armed conflicts "cyberwarfare." This situation changed after the 9/11 attacks. Today, it is known that terrorists use ICTs and the Internet for: propaganda; information gathering; preparation of real-world attacks; publication of training material; communication; terrorist financing; and attacks against critical infrastructure.
Cyber-laundering	The Internet is transforming money-laundering. Online financial services offer the option of enacting multiple, worldwide financial transactions very quickly. The Internet has helped overcome the dependence on physical monetary transactions. Surprisingly, stricter regulations to detect suspicious wire transfers have forced offenders to develop new techniques. The detection of suspicious transactions in the fight against money-laundering is based on obligations of the financial institutions involved in the transfer.
Phishing	Offenders have developed techniques to obtain personal information from users, ranging from spyware to "phishing" attacks. "Phishing" describes acts that are carried out to make victims disclose personal/secret information. Email-based phishing attacks contain three major phases. In the first phase, offenders identify legitimate companies offering online services and communicating electronically with customers whom they can target. Offenders design websites resembling the legitimate websites, "spoofing sites," requiring victims to perform normal log-in procedures, and enabling offenders to obtain personal information.



Hands Up, Online Gangs!

The World's Efforts in Cybersecurity

As the number of cybercrime offenses grows larger and larger, not only international organizations but also each nation is considering launching its own countermeasures against cybercrime. So, be aware, online criminals! Now is the time for you to shudder at those countermeasures against cybercrime.

AFRICA: Nigeria "National Cybersecurity Strategies"

Nigeria has persevered in its effort to keep its online society intact by setting up the National Cybersecurity Strategies in terms of five aspects that national measures must not forget to consider: awareness, legal reforms, institutional capacity building, public-private collaboration, and international law enforcement cooperation.

In order to increase public awareness and enhance capacity building, Nigeria covered all crucial areas through the press and organized relevant units of agencies such as cybercrime units and computer crime prosecution units. For legal reforms, the Nigerian government constituted the cybersecurity framework of the Nigerian Cybercrime Working Group, including Nigeria Police Force (NPF), the National Security Adviser (NSA), Nigeria Computer Society (NCS), etc., and drafted the bill titled "Computer Security and Critical Information Infrastructure." The legislation designates three kinds of acts as cybercrime: conduct against ICT systems; conduct using ICT systems to carry out unlawful activities or commit crimes; and unlawful conduct committed against critical information infrastructures.

Government-industry forum on lawful interception was prepared to seek the benefits of public-private partnership while the Nigerian Economic and Financial Crimes Commission participated in the G8 24/7 Network, although Nigeria is not a signatory member. For more information, please see: National Cybersecurity Strategies presented at Africa Regional Conference on Cybersecurity, Yamousoukro, Nov.17-20, 2008.

ASIA: Japan "Internet Hotline Center"

In Japan, cybersecurity is mainly dealt with by the Ministry of Internal Affairs and Communications (MIC) and the National Police Agency (NPA). Achieving u-Japan by 2010 is the MIC's goal, and within the policy package, there is an item of promoting 21 strategies for ICT's safety and security. Among the 21 strategies, Japan attempts to realize a highly reliable system to remove damages caused by cyber terrorism by manufacturing IPv6 information applications and investing in R&D on ultra high-speed satellite communication technologies and mobile satellite communication technologies. Additionally, promoting the use of anti-virus software as well as disseminating information regarding the experiences and damages of viruses by setting up more Websites are ways in which the MIC adheres in order to meet the goal of only 10% of Internet users confronting cyber attacks throughout the year. For the strategy to deal with junk mail, an amendment bill

concerning spam was drafted, and the use of technologies such as Outbound Port 25 Blocking (OP25B) to block spam has been supported.

On the other hand, the use of electronic signature and authentication, measures against bogus invoices, and reinforcement of complaint and advisory windows at telecommunication consumer advisory centers and local stations will bear fruit in reducing the number of online crimes and fraud to one-half by 2010. In the field of protecting intellectual property, the MIC executed the Intellectual Property Strategic Program in 2004 and has reinforced both bilateral and multilateral cooperation, including discussions on New Broadcasting Treaty with the World Intellectual Property Organization (WIPO).

The Japanese government saw that the cause of various crimes was the immeasurable illegal and harmful content on the Internet and thereby established the Internet Hotline Center in June 2006. Besides, inside of the NPA, the Cyber Forces (mobile technical units) were established in 2001. The unit works cooperatively with the Patent Prosecution Highway (PPH) in order to share information about information security and prepare for emergencies. For more information, visit: http://www.soumu.go.jp, http://www.npa.go.jp

EUROPE: Malta "The Smart Island"

When examining carefully Malta's National ICT Strategy for 2008-2010, we can observe that Malta stands on the basis of being a smart island. To attain its goal, the island emphasizes significantly on bringing the ICT environment to world-class. Thus, what Malta supports is formulating the smarter regulation of telecommunications and electronic services. This is also under the logic that the safer environment attracts more investors. This means that Malta will continue to be among the best prepared countries in legislative and regulatory terms for the changing needs of technology. All areas beginning from mobile and e-authentication to e-commerce, e-identification, and electronic signing and voting will be considered in formulating e-legislation for Malta.

This is not all. Malta government is also aware of the need to strengthen the Criminal Code's provisions against cybercrime. Corresponding to the need, the country plans to be a physical hub as well as an international hub for information security services through setting up adequate public and private infrastructure in Malta. When it comes to information security strategy, the Maltese government founded a national information security agency shifting the responsibility to closely be connected to industries to promptly react to e-security threats.

In particular, the island's focus of cyber security places on the safety for children. With the Commission for Children, the government works with public-private partners to develop a series of school safety packages on the purpose to educate and equip the children, teachers and parents with the technology they need to protect them from cybercrime. Furthermore, the cybercrime unit will be soon be established within the Malta Police Force.

For more information, visit: http://mitc.gov.mt

MIDDLE EAST: Egypt "Suzanne Mubarak Women's International Peace Movement (SMWIPM)"

The Egyptian government has joined the movement toward an information society since 2002 by embarking on a national project called the "Free Internet Initiative" as a part of the Information Society Initiative. At the same time, the Egypt PC 2010-Nation Online Initiative was launched with other national projects regarding the pursuit of the development of e-content and broadband accessibility.

In the process of the implementation of those national ICT projects, Egypt did not forget the importance of the security of online society. The Egyptian government worked hand in hand with international organizations and multinational corporations to implement the security strategies. The launch was opened by the Egypt's first lady, Mrs. Suzanne Mubarak. She founded the Suzanne Mubarak Women's International Peace Movement (SMWIPM) and set up the Cyber Peace Initiative in 2007. The movement called upon to the unification of law enforcement as well as an internationally coordinated cybercrime investigation training program for law enforcement agencies and industries. Furthermore, the organization is enthusiastic about holding the International Youth Forum in order to spread a culture of peace, tolerance and dialogue among the youth as well as protecting children from misuse of the Internet. For more information, visit: http://www.womenforpeace international.org, http://www.smwipm.cyberpeaceinitiative.org/en ICWT